FS-20191009.05C2

Microsoft Netherlands
Attn. ###############

Dutch Standardization Forum

Contact
info@forumstandaardisatie.nl

T +31-(0)70-888 7776

Date
30 August 2019

notitie

Information on Dutch government’s position on DNSSEC and DANE (for secure mail transport)

Copy to: Strategisch Leveranciersmanagement Rijk

Strategisch Leveranciersmanagement Rijk sent a letter to Microsoft regarding “Gebruik DANE en DNSSEC” on 31 July 2019. With this letter the Dutch government formally asked Microsoft to offer support for the mandatory standards DNSSEC and DANE on Office 365. In the meeting on the 23rd of August at the Dutch Ministry of Justice and Security this letter was discussed with you. With this note we provide you with more background information that you asked for in order to reply to the letter.

Summary

- Email transport can be secured with DANE (RFC 7672). DANE works on top of STARTTLS making it possible to enforce and authenticate transport encryption.
- DANE and underlying DNSSEC have been made mandatory within the Dutch government on the highest level. An implementation deadline has been set for the end of 2019.
- Many other Microsoft customers have asked for DANE and DNSSEC support as well.
- Several other countries also have active policies to promote DANE.
- Many vendors are moving towards DANE, and DANE adoption is steadily growing within and outside Dutch government.
- Microsoft Office 365 currently does not offer support for DANE. This means that Dutch government organizations that would use Microsoft Office 365 cannot be compliant with regulations and standards. This is a reason for government organizations being reluctant to use Office 365.
- In Q1 2020 the Standardization Forum will report to the OBDO and House of Parliament on the results and bottlenecks. We prefer to present a positive statement about DNSSEC and DANE support in Office 365.
- With the abovementioned letter the Dutch government has urged Microsoft to offer support DANE and DNSSEC and provide for a clear implementation timeline.

1. DANE mandatory for Dutch governments

Open standards policy

The Dutch government aims to protect the confidentiality and integrity of its communications between government institutions, with its citizens, and with other organizations and nations. Email is a very popular, yet inherently insecure, communication system. However, extensions to this distributed system have over time corrected some of its vulnerabilities, examples of such extensions being standards DKIM, SPF, DMARC, STARTTLS and DANE.

In order to benefit from the security upgrades these standards provide, these standards, including DANE and underlying DNSSEC, have been declared mandatory for government organizations. Imposing selected standards is done by the highest official, inter-administrative body on digital government policy (Overheidsbreed Beleidsoverleg Digitale Overheid, OBDO), that is advised by the Dutch Standardization Forum. This is part of the open standards policy that is in use since 2008[1]. In short, the policy dictates that when purchasing an IT service or IT product for an area of application that appears on an authoritative list of open standards, a government organization must opt for an IT service or an IT product that uses the relevant open standard specified in that application area. This list, including DANE, DNSSEC and other mandatory Internet security standards, can be found online[2].

Additional agreements on implementation deadlines

In addition the OBDO has agreed that all government organizations must have implemented anti-phishing email standards (DKIM/SPF/DMARC) and the standards against eavesdropping by email (STARTTLS and DANE) by the end of 2019. On December 21, 2018, the State Secretary for the Interior and Kingdom Relations has informed the House of Parliament about this agreement[3].

The Dutch Standardization Forum measures the progress of these agreements. The latest measurement shows that DNSSEC adoption is currently at 93% for government domains. DNSSEC adoption for email servers is at 71%, illustrating the dependency on email service providers. DANE adoption has nearly doubled in six months' time from 25% to 41%[4]. Non-support of DNSSEC and DANE in Office 365 is a bottleneck of about 10%. In Q1 2020 the Standardization Forum will report to the OBDO and House of Parliament on the results and bottlenecks, and our wish is to present a positive statement about DNSSEC and DANE support in Office 365.

Government information security baseline

The mandatory status of DANE and DNSSEC is also reflected in the government-wide information security baseline (Baseline Informatiebeveiliging Overheid) that was established by the Dutch Council of Ministers on December 14, 2018. Control

[1] https://wetten.overheid.nl/BWBR0024717/2008-11-23 (Dutch)

[2] https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht (Dutch)

[3] https://www.tweedekamer.nl/kamerstukken/detail?id=2018Z11914&did=2018D60719 (Dutch)

[4] https://www.forumstandaardisatie.nl/nieuws/groei-informatieveiligheidstandaarden-bij-overheid-maar-ook-werk-aan-de-winkel (Dutch)

13.2.3.1 in this baseline is requiring government organizations to use DANE and the underlying DNSSEC standard to protect email communications[5].

General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) requires data processors to ensure that appropriate technical and organizational measures have been implemented to secure personal data[6]. The Dutch Data Protection Authority (Dutch DPA) has provided guidance on appropriate technical and organizational measures on their website, where in case of email communications they refer to the Factsheet 'Secure the connections of mail servers' by the Dutch National Cyber Security Centre (NL-NCSC)[7]. In this factsheet NL-NCSC recommends enabling STARTTLS and DANE for all your organization's incoming and outgoing email traffic[8].

Healthcare sector

Furthermore DANE is part of the implementation guidelines of the Dutch technical agreement on mail security for the healthcare sector that has been published in May 2019.[9]

2. DANE market development

Request from other Microsoft customers

The Dutch government is not alone in its request for support for DNSSEC and DANE. On the Microsoft Azure Feedback Forums the feature request for DNSSEC support is the single most supported feature request in the Networking category. With over 3,200 votes it is the 6th most supported feature request out of 38,140 feature requests on the Microsoft Azure Feedback Forums[10]. On the Office 365 User Voice Forums, requests for DNSSEC and DANE support have been supported over 1,500 times, and the request is around the 30th most supported feature request of 21,441 feature requests[11].

Policy in other countries

- The German Federal Office for Information Security (BSI) published technical guidelines in publication 'BSI TR-03108-1:Secure E-Mail Transport' which require DANE for incoming and outgoing email traffic. The DPA of Nordrhein-

[5] https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html#d17e150 (Dutch)

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679 (English)

[7] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens/ (Dutch)

[8] https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers (English)

[9] https://www.nen.nl/NEN-Shop/Nieuwsberichten-Zorg-Welzijn/NTA-7516-Veilige-email-in-de-zorg-beschikbaar-voor-het-veld-1.htm (Dutch)

[10] https://feedback.azure.com/forums/217313-networking/suggestions/13284393-azure-dns-needs-dnssec-support (English)

[11] https://office365.uservoice.com/forums/273493-office-365-admin/suggestions/13415532-dnssec-support-in-office-365 and https://office365.uservoice.com/forums/289138-office-365-security-compliance/suggestions/32360299-dnssec-support-in-office-365 (English)

Westfalen (Germany) mandates email transport to be implemented according to these technical guidelines[12].

- The EU Multi Stakeholder Platform on ICT Standardisation evaluated and gave a positive advice to the identification of DANE for referencing in public procurement that was confirmed by the European Commission[13].
- The Norwegian government recommends the use of DANE for email transport security[14].
- The U.S. National Institute of Standards and Technology recommends DANE as a standard for enhancing trust in email[15].
- The Swedish and Dutch domain registries have incentive programs for DANE[16].

Adoption statistics and vendor support

The adoption of DANE has been growing steadily since its introduction in October 2015. Currently over 1.2 million domains are DANE-enabled.[17]

More and more vendors offer support for DANE. Publication of DANE records (and the underlying DNSSEC) is supported by several DNS providers including Cloudflare and Google Domains. We have also seen mail server software support outbound DANE verification, currently a.o. Cisco ESA, Postfix, Cloudmark, Halon, Exim and Port25 PowerMTA. And lately Proofpoint publicly announced they work on DANE verification support. Furthermore a growing number of mail providers support DANE, like Comcast, One.com, GMX, XS4ALL, Posteo and Mailbox.org. Google lately started to offer DNSSEC-signed domains for their Gsuite mail servers to customers, seemingly paving the road for DANE support as a next step.

We are aware of MTA-STS. This is a very new standard with which there is little experience (especially outside the big cloud mail providers). Moreover, MTA-STS is less secure than DANE (because of 'trust on first use') which is acknowledged in the MTA-STS specification. Both standards are not mutually exclusive. In short: despite MTA-STS, in our opinion DANE remains very relevant.

3. Closing remarks

The Dutch government considers DANE and underlying DNSSEC as essential standards in order to protect email communications. Both standards have been made mandatory within the Dutch government on the highest level. Dutch government organizations are to procure and implement systems that use these open standards over systems that do not. An implementation deadline has been set for the end of 2019. In Q1 2020 the Standardization Forum will report to the OBDO and House of Parliament on the results and bottlenecks, and we would like to present a positive statement about DNSSEC and DANE support in Office 365.

[12] https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand.html (German)

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1515759784644&uri=CELEX:32017D2288 (English)

[14] https://www.difi.no/referansekatalogen/grunnleggende-datakommunikasjon (Norwegian)

[15] https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/final (English)

[16] https://lists.dns-oarc.net/pipermail/dns-operations/2018-November/018127.html (English) and https://www.sidn.nl/nieuws-en-blogs/nieuwe-stimulans-voor-beveiligingsstandaarden-dnssec-en-dane (Dutch)

[17] http://stats.dnssec-tools.org/#graphs and https://github.com/baknu/DANE-for-SMTP/wiki