INFORMATIE
BEVEILIGINGS
DIENST

STARTTLS EN DANE: WEB- EN E-MAILVERKEER BESCHERMEN

Met STARTTLS en DANE wordt een betrouwbare e-mailcommunicatie tussen gemeenten en burgers, bedrijven, (keten)partners en (semi)overheidsorganisaties bevorderd en beschermt de gemeente zichzelf tegen het afluisteren en manipuleren van e-mailberichten. Dit geldt voor alle domeinnamen, waarvan de gemeente de houder is. De toepassing van STARTTLS in combinatie met DANE zorgt ervoor dat de verzendende e-mail client applicatie zekerheid heeft dat met de juiste inkomende e-mailserver verbonden is, en dat de verbinding met TLS beveiligd is. DANE voorkomt aanvallen waarbij een aanvaller zich uitgeeft voor de inkomende e-mailserver en STARTTLS blokkeert om zo toegang tot de onversleutelde berichten te krijgen of berichten te vervalsen. Deze factsheet biedt gemeenten informatie over de standaarden en de manier waarop deze kunnen worden geïmplementeerd.

Versleutelde communicatie op het internet maakt meestal gebruik van Transport Layer Security (TLS).[1] TLS is afhankelijk van derde partijen om de geldigheid van de sleutels die gebruikt worden te garanderen. Het DNS-based Authentication of Named Entities (DANE) protocol verbetert deze situatie doordat de domeinnaambeheerder de digitale certificaten die voor het opzetten van de versleutelde communicatie, voor het domein, zelf kan specificeren. DANE bindt hiervoor de digitale certificaten[2] aan domeinnamen. Informatie over de legitieme digitale certificaten dienen daarvoor in het DNS-systeem opgenomen te worden. DANE bouwt voort op Domain Name System Security Extensions (DNSSEC)[3] en wordt met name gebruikt bij het veilig uitwisseling van webverkeer, via HyperText Transfer Protocol Secure (HTTPS), en de beveiliging van e-mailverkeer, via Simple Mail Transfer Protocol (SMTP). DANE kan breder ingezet worden, maar dat laten we in deze factsheet buiten beschouwing. DANE heeft belangrijke voordelen ten opzichte van het huidige digitale certificatensysteem.[4]

STARTTLS is een uitbreiding op de SMTP-standaard waarmee het mogelijk wordt om SMTP-verkeer over een met TLS versleutelde verbinding te laten lopen. Door deze STARTTLS uitbreiding wordt een niet-versleutelde, en daarmee onbeveiligde, verbinding opgewaardeerd naar een met TLS versleutelde verbinding.

Op de website internet.nl kunt u eenvoudig controleren of uw gemeente-website gebruik maakt van een versleutelde verbinding, zodat de verbinding tussen een clientapplicatie (browser) en de gemeente-webserver niet kan worden afgeluisterd of gemanipuleerd. Tevens wordt gecontroleerd of gebruik wordt gemaakt van DANE, deze controle wordt ook uitgevoerd voor uw gemeentelijke e-maildomein.[5] Hierdoor wordt op betrouwbare wijze duidelijk gemaakt dat uw web- en e-mailserver via een beveiligde verbinding bereikbaar zijn. Deze factsheet richt zich op de methode om op een betrouwbare wijze duidelijk te maken dat uw web- en e-mailserver(s) via een beveiligde verbinding, via TLS en STARTTLS[6], bereikbaar zijn. In deze factsheet wordt achtereenvolgens aandacht besteed aan het huidige digitale certificatensysteem en het nadeel van dit certificatensysteem, de beveiligingsvoordelen van STARTTLS en DANE voor gemeenten, de STARTTLS en DANE-standaard, hoe uw gemeente gebruik kan maken

1 Zie hiervoor de factsheet 'TLS zorgt voor veilige verbinding met de gemeentewebsite' van de IBD
2 Aangeduid met X.509. Een X.509 certificaat is een digitaal certificaat dat de algemeen aanvaarde internationale X.509 Public Key Infrastructure (PKI) standaard gebruikt om te controleren of een publieke sleutel toebehoort aan de identiteit (bijvoorbeeld gebruiker, computer of dienst) die is opgenomen in het digitale certificaat (https://tools.ietf.org/html/rfc5280)
3 Zie hiervoor de factsheet 'DNSSEC: voorkom domeinnaamfraude' van de IBD
4 Ook wel X.509 Public Key Infrastructure (PKI; PKIX) genoemd

STARTTLS EN DANE ZORGEN IN COMBINATIE VOOR VERSLEUTELDE EN GEVERIFIEERDE VERBINDING TUSSEN MAILSERVERS

5 Er wordt gecontroleerd of er TLSA-record in de DNS is opgenomen voor het betreffende domein
6 Als inkomende e-mailservers STARTTLS ondersteunen, dan kunnen uitgaande e-mailservers met deze inkomende e-mailserver een beveiligde verbinding opzetten die ervoor zorgt dat (passieve) aanvallers e-mailberichten niet kunnen afluisteren

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

van STARTTLS en DANE en tenslotte het IBD advies. Deze factsheet geeft uitgebreidere en meer technische achtergrondinformatie dan de korte versie van deze factsheet die ook beschikbaar is op de website van de IBD.

Verhogen vertrouwen in gemeentelijke domeinnaam

De toepassing van STARTTLS in combinatie met DANE zorgt ervoor dat de verzendende e-mail clientapplicatie zekerheid heeft dat met de juiste inkomende e-mailserver verbonden is, en dat de verbinding met TLS beveiligd is. DANE voorkomt aanvallen waarbij een aanvaller zich uitgeeft voor de inkomende e-mailserver en STARTTLS blokkeert om zo toegang tot de onversleutelde berichten te krijgen of berichten te vervalsen.
Met STARTTLS en DANE wordt een betrouwbare e-mailcommunicatie tussen gemeenten en burgers, bedrijven, (keten)partners en (semi)overheidsorganisaties bevorderd en beschermt de gemeente zichzelf tegen het afluisteren en manipuleren van e-mailberichten. Dit geldt voor alle domeinnamen, waarvan de gemeente de houder is.

Concreet betekent dit dat STARTTLS en DANE ervoor zorgt dat uw gemeente:

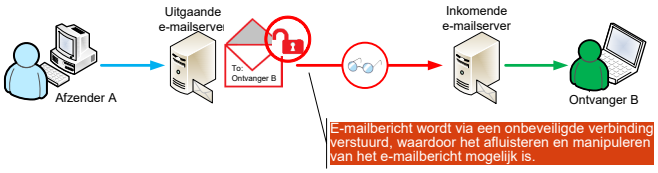
- De kans vermindert dat derden het gebruik van STARTTLS te blokkeren waardoor de verbinding niet versleuteld wordt en het e-mailberichtenverkeer kan worden onderschept.
- De zekerheid vergroot, dat de authenticiteit van de server en of de server-to-server verbinding legitiem is en niet wordt gemanipuleerd.

Voldoen aan wet- en regelgeving

In sommige gevallen is het gebruik van versleutelde verbindingen verplicht. Deze verplichting kan gesteld zijn in het informatiebeveiligingsbeleid van uw gemeente, maar ook in wet- of regelgeving. De Wet bescherming persoonsgegevens (Wbp) kent een brede verplichting (artikel 13) om persoonsgegevens afdoende te beveiligen. In de Richtsnoeren beveiliging van persoonsgegevens van de Autoriteit Persoonsgegevens (AP) staat gespecificeerd dat bij verzending van persoonsgegevens via het internet, dus ook via e-mail, in veel gevallen versleutelde verbindingen (TLS) wordt vereist. Deze vereiste speelt voor gemeenten omdat veel uitgewisselde gegevens persoonsgegevens zijn.
De STARTTLS en DANE-standaard zijn sinds 2016, voor het beveiligen van e-mailverkeer[7], opgenomen op de lijst met verplichte open standaarden voor de gehele publieke sector (‘pas-toe-of-leg-uit-lijst’) van het Forum Standaardisatie. Dit betekent dat overheden en semi-overheden STARTTLS en DANE dienen toe te passen en alleen in geval van zwaarwegende redenen daarvan mogen afwijken. Tevens adviseert het Nationaal Cyber Security Centrum (NCSC) om STARTTLS en DANE in te schakelen voor al het inkomende en uitgaande e-mailverkeer van uw organisatie.[8]

WAT LEVERT STARTTLS MIJN GEMEENTE OP?

E-mailberichten worden door de e-mailserver van de verzendende partij verstuurd naar de e-mailserver van de ontvangende partij op basis van de Simple Mail Transfer Protocol (SMTP)-standaard[9]. SMTP werkt zowel over beveiligde als onbeveiligde verbindingen, maar standaard gebeurt dit zonder versleuteling of beveiliging, waardoor het afluisteren en manipuleren van e-mailberichten mogelijk is (zie Figuur 1).



Figuur 1 E-mailbericht via onbeveiligde verbinding.

Door (strengere) privacywetgeving en de toename van cybercriminaliteit wordt het steeds belangrijker dat e-mailservers gebruikmaken van met TLS versleutelde verbinding voor het transport van e-mailberichten. Het is mogelijk om e-mailverkeer te versleutelen met TLS, dezelfde standaard die ook gebruikt wordt voor het versleutelen van webverkeer (HTTPS). Een inkomende (ontvangende) e-mailserver kan aangeven over deze mogelijkheid te beschikken en met STARTTLS[10] kan de uitgaande (verzendende) e-mailserver aangeven van deze mogelijkheid gebruik te willen maken. STARTTLS is een uitbreiding op de SMTP-standaard waarmee het mogelijk wordt om SMTP-verkeer over een met TLS versleutelde verbinding te laten lopen. Door deze STARTTLS uitbreiding wordt een niet-versleutelde, en daarmee onbeveiligde, verbinding opgewaardeerd naar een met TLS versleutelde verbinding. Hierdoor wordt voorkomen dat een passieve aanvaller[11] het e-mailberichtenverkeer kan afluisteren.
Let op: STARTTLS zorgt voor een versleuteling op verbindingsniveau en niet voor een versleuteling op berichtniveau, zoals dat bij Secure/Multipurpose Internet Mail Extensions (S/MIME)[12] dat het geval is.
STARTTLS wordt door de meeste e-mailservers ondersteund, zoals de populaire Unix en Linux e-mailservers, sendmail[13], qmail[14] en postfix[15], evenals Microsoft Exchange[16]. Om STARTTLS te laten werken is het noodzakelijk dat zowel de uitgaande als inkomende e-mailserver STARTTLS ondersteunt.
Het transparantierapport van Google geeft onder andere inzicht in hoeveel e-mailberichten die zijn uitgewisseld tussen Gmail en andere providers, e-mailversleuteling toepassen terwijl deze worden verzonden via internet.[17] Het geeft inzicht welke e-mailservers van verzendende en ontvangende organisaties STARTTLS ondersteunen.

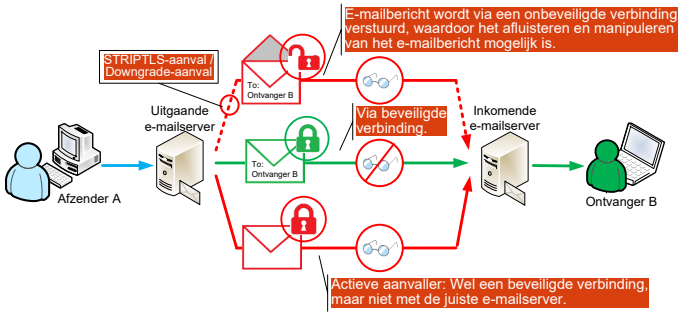
Manipuleren van e-mailberichtenverkeer

Wanneer STARTTLS door één van de e-mailservers niet wordt ondersteund of een versleutelde verbinding om

7 De verplichting om STARTTLS en DANE alleen voor het beveiligen van e-mailverkeer toe te passen heeft te maken met het feit dat DANE door de meeste client applicaties (bijvoorbeeld webbrowsers) op dit moment nog niet standaard ondersteund wordt. Hiervoor dient gebruik gemaakt te worden van externe add-ons/plug-ins
8 Zie hiervoor ook de factsheet ‘Beveilig verbindingen van mailservers’ van het NCSC: https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-verbindingen-van-mailservers.html

9 https://tools.ietf.org/html/rfc5321
10 https://tools.ietf.org/html/rfc3207
11 passieve en actieve aanval: Een passieve aanvaller is een aanvaller de netwerkverbindingen afluistert maar de inhoud ervan niet verandert/manipuleert. Een actieve aanvaller verandert/manipuleert daarentegen het netwerkverkeer dus wel
12 https://tools.ietf.org/html/rfc3851
13 http://www.sendmail.com/
14 http://www.qmail.org/top.html
15 http://www.postfix.org/
16 https://products.office.com/nl-nl/exchange/email
17 https://www.google.com/transparencyreport/saferemail/?hl=nl

een andere reden niet tot stand kan worden gebracht, wordt automatisch teruggevallen op een niet-versleutelde verbinding (achterwaarts compatibel). Er wordt geen TLS afgedwongen, zoals bij HTTPS. Dit wordt opportunistische versleuteling genoemd. Door het terugvallen op een onbeveiligde verbinding wordt voorkomen dat STARTTLS een negatieve invloed heeft op de afleveringszekerheid van e-mailberichten. Dit is echter wel een nadeel voor de vertrouwelijkheid en integriteit van e-mailverkeer. Dit geeft actieve aanvallers[18] de mogelijkheid om het gebruik van STARTTLS, via een STRIPTLS-aanval, te blokkeren waardoor de verbinding niet versleuteld wordt en e-mailberichten kunnen worden onderschept (zie Figuur 2). Dit wordt ook wel een downgrade-aanval[19] genoemd. Een actieve aanvaller kan het e-mailberichtenverkeer manipuleren. Het tot stand brengen van een beveiligde TLS-verbinding met STARTTLS gebeurt via een niet-versleutelde verbinding. Door in het beginstadium het aanbod van een versleutelde verbinding te blokkeren, gaat de uitgaande e-mailserver er vanuit dat TLS niet beschikbaar is. De uitgaande e-mailserver gaat dan verder met de niet-versleutelde verbinding. Door deze manipulatie van het e-mailberichtenverkeer is het voor actieve aanvallers mogelijk om de verbinding af te luisteren en de e-mailberichten te lezen.



Figuur 2 E-mailverkeer met gebruik van TLS en STARTTLS

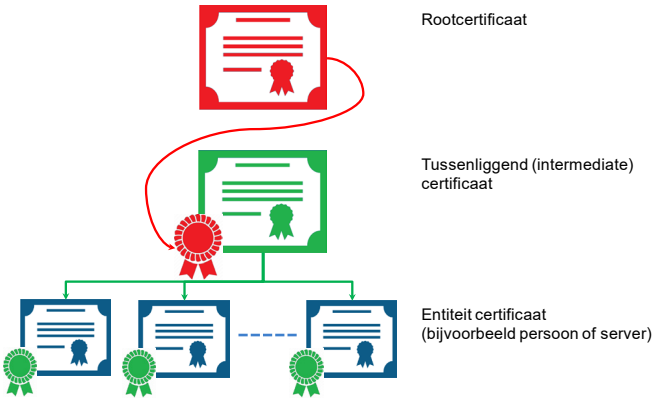
Dat STRIPTLS-aanvallen niet alleen theoretisch mogelijk zijn maar ook daadwerkelijk in de praktijk voorkomen is in 2015 door onderzoekers aangetoond[20] en de resultaten van het onderzoek zijn tijdens 'The 2015 Internet Measurement Conference (IMC)' gepresenteerd.
Naast het blokkeren van STARTTLS door een actieve aanvaller kan een actieve aanvaller ook het e-mailberichtenverkeer manipuleren door het e-mailberichtenverkeer om te leiden naar een andere (niet juiste) e-mailserver. Bij deze aanval wordt wel een beveiligde verbinding opgezet, maar met een (vals) digitaal certificaat, die door de actieve aanvaller wordt geleverd.

Het huidige digitale certificatensysteem

Bij het maken van een veilige verbinding naar een onbekende partij is een online controle op de authenticiteit van de verzendende partij en de eindbestemming wenselijk. Dit kan door middel van een (gepubliceerd) digitaal certificaat die door een certificaatautoriteit (CA), de certificaatuitgever, is uitgegeven. Om digitale certificaten te kunnen genereren, registreren, distribueren, valideren en beheren is een infrastructuur nodig. Die wordt de Public Key Infrastructure (PKI) genoemd.[21] De PKI is een infrastructuur voor vertrouwen en bestaat uit meer dan techniek alleen. Het omvat ook processen, procedures, organisaties en spelregels waar men zich aan dient te houden.

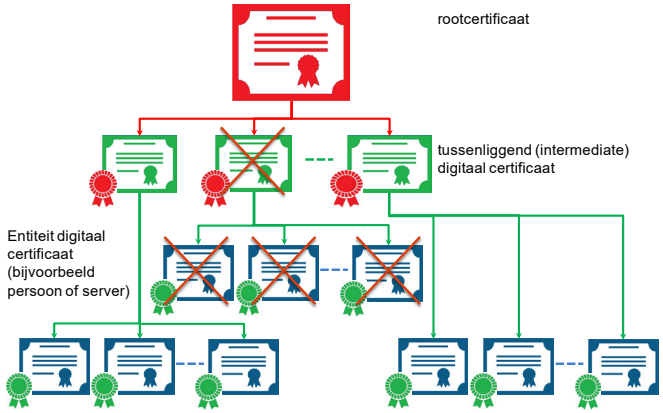
De beveiliging van het digitale certificatensysteem is gebaseerd op een vertrouwensketen, de chain of trust. Deze vertrouwensketen loopt van de CA, de certificaatuitgever, tot aan het eigen gemeentelijke digitale certificaat en alle tussenliggende niveaus. Een digitaal certificaat is een combinatie van identiteit en publieke sleutel die gewaarmerkt is door de CA. Het digitale certificaat wordt rechtstreeks door de clientapplicatie (bijvoorbeeld een browser) geverifieerd. Het digitale certificaat wordt door de clientapplicatie aanvaard als het door een vertrouwde uitgevende CA digitaal is ondertekend.[22] Tientallen verschillende CAs zijn in client applicaties (bijvoorbeeld browsers) opgenomen, middels het rootcertificaat[23] van de CAs, en deze zijn automatische door de leverancier van de clientapplicatie meegeleverd. Zonder dit rootcertificaat aanvaard de clientapplicatie het digitale certificaat niet, omdat de CA die het digitale certificaat heeft uitgegeven niet bekend is. De clientapplicatie zal op dat moment een waarschuwing tonen en aan de gebruiker vragen wat nu te doen. De verbinding weigeren/verbreken of de verbinding toch opzetten zonder dat het digitale certificaat gecontroleerd kan worden. Browserontwikkelaars dragen zorg dat bij updates de verouderde of vervallen digitale certificaten automatisch vervangen worden door nieuwe.

Een CA dient aan strenge veiligheidseisen te voldoen om te garanderen dat hun digitale certificaten niet gecompromitteerd worden. Naast het huidige rootcertificaat, waarvan de privé sleutel streng bewaakt wordt, en die vaak niet gebruikt wordt om digitale entiteit[24] certificaten rechtstreeks digitaal te ondertekenen, maken certificaatuitgevers gebruik van tussenliggende (intermediate) certificaten, vaak één per product of dienst (zie Figuur 3). Mocht de privé sleutel van één van deze tussenliggende digitale certificaten gecompromitteerd worden, dan is daarmee nog steeds de veiligheid gegarandeerd van digitale entiteit certificaten die door een ander tussenliggend CA uitgegeven zijn (zie Figuur 4).



Figuur 3 Certificeringsboom

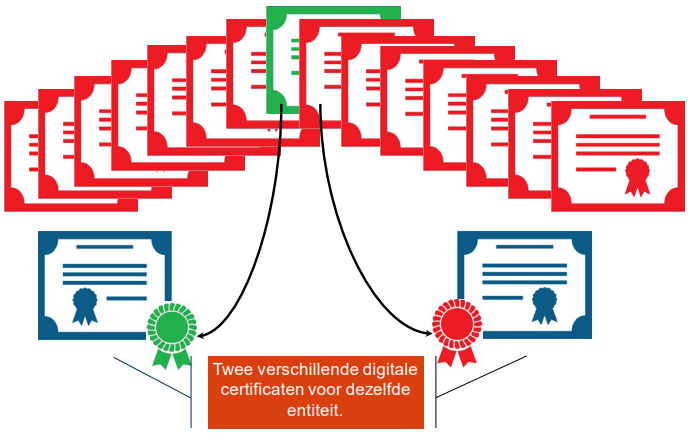
18 De actieve aanvaller voert hiervoor een man-in-the-middle (MITM)-aanval uit. Dit is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de aanvaller zich tussen de twee communicerende partijen. De e-mailberichten kunnen daarbij mogelijk gelezen en veranderd worden. Ook kunnen e-mailberichten worden verzonden die niet door de andere partij zijn geschreven
19 Een andere vorm van een downgrade-aanval is dat de actieve aanvaller het berichtenverkeer manipuleert door de versleutelingsterkte te verlagen (https://en.wikipedia.org/wiki/Downgrade_attack)
20 Bron: Neither Snow Nor Rain Nor MITM...: An Empirical Analysis of Email Delivery Security, https://dl.acm.org/citation.cfm?id=2815695. of https://www.elie.net/publication/neither-snow-nor-rain-nor-mitm-an-empirical-analysis-of-email-delivery-security
21 Zie hiervoor het operationele BIG product 'Encryptiebeleid (PKI)' van de IBD
22 Zie hiervoor de whitepaper 'Understanding Certification Path Construction' van het PKI Forum (http://www.oasis-pki.org/pdfs/Understanding_Path_construction-DS2.pdf)
23 Een rootcertificaat is een zelf-ondertekend digitaal certificaat die de uitgevende certificaatautoriteit identificeert
24 Een entiteit kan bijvoorbeeld een persoon, afdeling, een naam van een domein, server of host zijn



Figuur 4 Certificeringsboom met ongeldig tussenliggend digitaal certificaat

Huidig probleem met het digitale certificatensysteem

In het huidige digitale certificatensysteem worden de digitale servercertificaten direct geverifieerd door de client applicatie. Alle daarvoor benodigde rootcertificaten worden met de clientapplicatie meegeleverd. In principe kunnen meerdere organisaties een digitaal certificaat aanvragen, bij verschillende CAs, voor eenzelfde product of dienst (zie Figuur 5). Als deze verschillende CAs door de clientapplicatie worden vertrouwd dan kunnen beide digitale certificaten voor dat ene product of dienst worden gebruikt. Dit kan een legitieme reden hebben. Een organisatie kan bijvoorbeeld een tweede digitale certificaat, als extra set of 'back-up', aanschaffen voor één en hetzelfde product of dienst. Bijvoorbeeld om weer snel in bedrijf te zijn als het root- of tussenliggende digitaal certificaat van de primaire CA is gecompromitteerd, dan is er een snelle uitwijkmogelijkheid. Dit voorkomt (langdurige) disruptie van de dienstverlening door risicospreiding. Het kan uiteraard ook een minder legitieme reden hebben. Een kwaadwillende wil zich voordoen als degene die het product of dienst levert. Hiervoor vraagt deze kwaadwillende een digitaal certificaat aan met uw identiteit en een andere publieke sleutel. Daarna zorgt deze kwaadwillende ervoor dat uw dienstverlening niet meer bereikbaar is, bijvoorbeeld door DNS-spoofing[25], en dat uw product of dienst vanaf zijn 'nep' omgeving wordt aangeboden. Vanwege het geldige digitale certificaat denken gebruikers, van deze 'nep' omgeving, verbinding te hebben met uw (legitieme) omgeving in plaats van deze 'nep' omgeving van de kwaadwillende. De clientapplicatie accepteert het digitale certificaat aangezien het door een vertrouwde CA is uitgegeven.



Figuur 5 Twee (eind) entiteit certificaten van verschillende CAs voor hetzelfde product of dienst

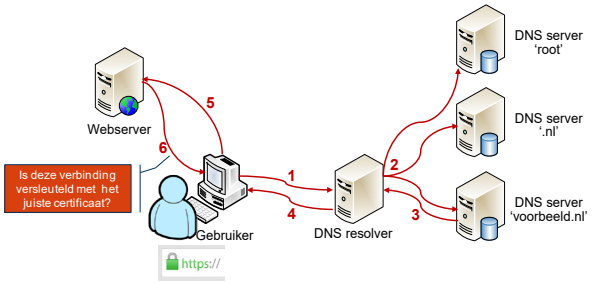
In Figuur 6 worden de stappen weergegeven die bij het opzetten van een versleutelde TLS verbinding worden doorlopen. Deze stappen zijn voor het webadres 'voorbeeld.nl':

1. De clientapplicatie wil een veilige verbinding (HTTPS) opzetten met website 'voorbeeld.nl. Hiervoor dient de clientapplicatie te achterhalen wat het IP-adres is van 'voorbeeld.nl'. Hiervoor wordt door de clientapplicatie een uitvraag gedaan bij de DNS-resolver.[26]
2. De DNS-resolver voert nu een uitvraag bij verschillende DNS-servers uit. Respectievelijk de 'root', '.nl' en de 'voorbeeld.nl' DNS-server.
3. De DNS-server waar de domeinnaam 'voorbeeld.nl' is geregistreerd geeft het IP-adres 10.2.1.125 terug aan de DNS-resolver.
4. De DNS-resolver retourneert het IP-adres 10.1.1.125 aan de clientapplicatie die het verzoek heeft ingediend.
5. De clientapplicatie zet nu een veilige (HTTPS) verbinding op met de website 'voorbeeld.nl'.
6. De gegevens van de webpagina worden nu via een TLS-versleutelde verbinding (Tunnel) uitgewisseld tussen de achterliggende webserver en client applicatie.

De vraag die nu blijft is of de verbinding is opgezet met de gegevens uit het officiële digitale certificaat dat bij het domein 'voorbeeld.nl' hoort. Het digitale servercertificaat is het startpunt voor verdere verificatie via de tussenliggende en rootcertificaten. Als een kwaadwillende (man-in-the-middle) onderweg het servercertificaat vervangt door een eigen digitaal certificaat dat de kwaadwillende via een van de CAs heeft weten te vervalsen, dan is dat voor een clientapplicatie nu voldoende om een beveiligde verbinding naar de server op te zetten. Omdat voor de clientapplicatie alles in orde lijkt, zal de clientapplicatie zonder waarschuwingen de verbinding opzetten.
De afgelopen jaren hebben verschillende hack incidenten bij CAs aangetoond dat een dergelijk vertrouwen in de vertrouwensketen de Public Key Infrastructure (PKI)-infrastructuur kwetsbaar maakt. Als een CA eenmaal is gehackt, dan moeten alle bijbehorende digitale certificaten ingetrokken en vervangen worden. Het 'Diginotarincident'[27], waarbij via een hack bij het Nederlandse bedrijf DigiNotar in juli 2011 een externe partij de gelegenheid kreeg meer dan 500 valse digitale certificaten te genereren en verspreiden. Deze hack, tezamen met andere hack incidenten zoals Comodo[28] en Flame[29], hebben geleerd dat misbruik (vervalsen) van digitale certificaten geen fictie maar realiteit is.

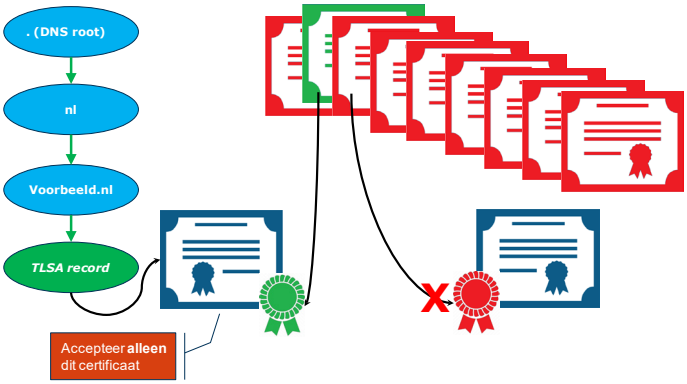
25 Het is namelijk mogelijk om het antwoord van de DNS te manipuleren, zodat een domeinnaam niet meer naar het juiste IP-adres verwijst. Hierdoor kunnen gebruikers op een verkeerde/malafide plaats terechtkomen

26 De DNS-resolver is de server waar client applicaties hun DNS-vragen aan stellen
27 Zie https://www.onderzoeksraad.nl/nl/onderzoek/1094/het-diginotarincident/fase/1256/onderzoek-diginotar-digitale-veiligheid-overheid-moet-sterk-verbeteren en https://www.rijksoverheid.nl/documenten/rapporten/2011/09/05/diginotar-public-report-version-1
28 Zie https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html
29 Zie https://technet.microsoft.com/library/security/2718704



1. Wat is het IP-adres van 'voorbeeld.nl'?
2. Uitvraag bij de verschillende DNS-servers
3. IP-adres van 'voorbeeld.nl' is 10.2.1.125
4. 10.1.1.125
5. https://voorbeeld.nl/
6. Webpagina via TLS-versleutelde verbinding (Tunnel)

Figuur 6 Typische TLS web interactie.



Figuur 7 DANE en PKI vertrouwensketen

Behalve de kwetsbaarheid van een gecentraliseerd digitaal certificatensysteem is een andere kwetsbaarheid dat een digitaal servercertificaat via dezelfde verbinding (in-band[30]) wordt verzonden. Nu is bij de clientapplicatie niet bekend door welke CA een servercertificaat digitaal ondertekend zou moeten zijn. Dat kun je alleen zien (maar niet verifiëren!) aan het digitale certificaat zelf op het moment dat de verbinding wordt gemaakt met de betreffende server.

WAT LEVERT DANE MIJN GEMEENTE OP?

DANE biedt een veiligheidsinfrastructuur naast PKI en voorziet versleutelde internetverbindingen van een extra beveiliging. Met deze aanpak wordt het hele systeem van digitale sleutels en certificaten veel robuuster. De huidige opzet is slechts zo veilig als de zwakste CA. DANE maakt het voor de eigenaar van een domein mogelijk om via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline digitale certificaten aan te reiken. Hierdoor kan realtime een controle worden gedaan op de authenticiteit van de server en of de server-to-server verbinding legitiem is en niet wordt gemanipuleerd. DANE is met name belangrijk tegen actieve aanvallers. Voor DANE dient het DNS-systeem uitgebreid te worden met een Transport Layer Security Association (TLSA) record.[31] Dit TLSA-record wordt gebruikt om in de DNS voor een domein aan te geven welke digitale sleutel/certificaat het juiste is en kan gezien worden als een digitale vingerafdruk/hashwaarde (zie Figuur 7). Op deze manier kan het digitale certificaat via DNS worden geverifieerd. Hierdoor kan het naast (of in plaats van) de digitale certificaten van CAs worden gebruikt. Komt de vingerafdruk/hashwaarde van het digitale certificaat niet overeen met de vingerafdruk/hashwaarde in het TLSA-record, dan is de verbinding niet te vertrouwen. Dit kan zowel de vingerafdruk/hashwaarde van een root als (eind) entiteit certificaat zijn. DANE biedt hierdoor realtime validatie per (individueel) digitaal certificaat, in plaats van offline per CA.

Als het digitale servercertificaat met de, door DNSSEC beveiligd, DNS-informatie wordt vergeleken (out-of-band), ziet de clientapplicatie direct dat het aangeboden digitale servercertificaat niet overeenkomt met de informatie uit het TLSA-record (zie Figuur 8). En daarmee is deze verbinding onbetrouwbaar en onveilig. De clientapplicatie (bijvoorbeeld browser) verifieert dan niet alleen of er sprake is van een geldig digitaal certificaat; er wordt ook geverifieerd of het bewuste digitale certificaat daadwerkelijk bij de betreffende domeinnaam (website) hoort. Het TLSA-record vormt op deze manier een additionele vertrouwensketen voor de digitale certificaten die voor het opzetten van TLS-verbindingen worden gebruikt. Het gebruik van DNSSEC is een verplicht onderdeel van DANE.[32] En omdat de informatie in de DNS is ondertekend met DNSSEC wordt het gebruik maken van valse digitale certificaten haast onmogelijk.
DANE wordt door de volgende e-mailservers ondersteund, zoals:postfix ondersteuning sinds 2014 (aanbevolen wordt versie 3.1 of later) ,halon[33] ondersteuning sinds 2015, exim[34] 4.85 (experimenteel), sendmail (geen ondersteuning maar er is een patch beschikbaar[35]) en Microsoft Exchange (geen directe ondersteuning maar via een oplossing van een derde partij XWall/CryptoFilter[36]).

EIGEN GEMEENTELIJKE PKI

Een gemeente zou kunnen overwegen om DANE te gebruiken als vervanger van de digitale (CA) certificaten. De gemeente hoeft dan geen digitaal certificaat bij een root-CA aan te schaffen, maar genereert dan een door de gemeente zelf-ondertekend digitaal certificaat (self-signed certificaat), dat tot nu toe een waarschuwing in de clientapplicatie (bijvoorbeeld browser) oplevert. Deze waarschuwing wordt getoond omdat de clientapplicatie het gemeentelijke rootcertificaat niet kan verifiëren, het gemeentelijke rootcertificaat is namelijk niet standaard in de clientapplicatie opgenomen. Op het moment dat de gemeente voor deze oplossing kiest dient de gemeente wel over een eigen gemeentelijk PKI te beschikken. De meeste gemeenten beschikken echter niet over een eigen PKI en zijn hiervoor afhankelijk van derden.

Het TLSA-record

Het TLSA-record is een record dat wordt gebruikt voor de DNS gebaseerde authenticatie van Named Entities en is speciaal voor DANE aan de DNS-standaard toegevoegd. In het TLSA-record wordt onder andere een vingerafdruk/hashwaarde van een digitaal (TLS) servercertificaten en informatie over de gebruikte cryptografische protocollen vastgelegd. Het

30 In computernetwerken worden out-of-band gegevens overgedragen via een transportkanaal dat onafhankelijk is van het in-band (hoofd) transportkanaal. Dit out-of-band mechanisme zorgt voor een conceptueel onafhankelijke kanaal, waardoor alle gegevens die via dat mechanisme worden verzonden van de in-band gegevens gescheiden worden gehouden
31 Voor implementatiediscussies/tips zie https://mail.sys4.de/pipermail/dane-users/
32 Zie https://tools.ietf.org/html/rfc6698
33 https://halon.io/
34 http://www.exim.org/
35 http://www.five-ten-sg.com/util/sendmail-8.16.0-dane.patch
36 Zie http://www.dataenter.com/doc/cryptofilter.htm

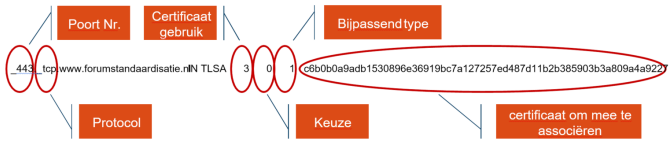
associeert (koppelt) een digitaal (TLS) servercertificaat of publieke sleutel, in de vorm van een vingerafdruk/hashwaarde, met de domeinnaam waar het TLSA-record is toegevoegd. Hierdoor wordt een 'TLSA certificate association' gevormd. Op deze manier kan van elke internetdienst de authenticiteit van het digitaal (TLS) servercertificaat via DNS worden geverifieerd, deze verificatie vindt plaats met het DANE-protocol. Het maakt het mogelijk om naast de offline digitale (TLS) certificaat verificatie een tweede, realtime, verificatie van het digitale (TLS) certificaat uit te voeren. Dit kan door:

- het specificeren van beperkingen waardoor een CA kan instaan voor een digitaal certificaat, of welk specifiek PKIX (eind) entiteit certificaat geldig is.
- het specificeren dat een dienstcertificaat of een CA direct kan worden geverifieerd in de DNS zelf.

Er wordt onderscheid gemaakt tussen het controleren van de certificaatautoriteit (CA) en het digitale certificaat en tussen het wel of niet controleren van de (gehele) vertrouwensketen. Vertrouwensketen verificatie betekent dat de geldigheid van het digitale (TLS) certificaat zelf wordt gecontroleerd.
Met DANE kan gebruik worden gemaakt van 'niet officieel' erkende zelfondertekende digitale certificaten, in deze situatie wordt de verificatie gedekt door DNSSEC in plaats van de CA. Dit is afhankelijk van de keuzes die worden gemaakt bij het genereren van het TLSA-record.

TLSA Resource Record (RR)

Het TLSA Resource Record (RR) wordt opgenomen in een door DNSSEC ondertekende zone, en bevat de informatie van het digitale (TLS) certificaat die overeenkomt met een specifieke dienst op een specifieke poort van de domeinnaam in die zone. Zoals weergegeven in Figuur 8 bestaat de RDATA (RR specifieke gegevens) voor een TLSA RR uit een 'certificaat gebruik', 'keuze' en een 'bijpassend type' veld en het gegevensveld waarmee het digitaal (TLS) certificaat moet worden geassocieerd.



Figuur 8 TLSA Resource Record (RR) voor www.forumstandaardisatie.nl

Het gegevensveld met de informatie van het digitaal certificaat (de payload van het TLSA RR) wordt geassocieerd met het digitale (TLS) certificaat dat door de (web)server wordt aangeboden. De velden gebruik, keuze en bijpassend type bepaalt hoe de vergelijking tussen de payload en het digitale (TLS) certificaat van de (web)server wordt uitgevoerd.
In Figuur 9 wordt het resultaat weergegeven van een DANE controle van een TLS dienst.[37] Hierbij wordt een verbinding opgezet met de ingegeven dienst (in Figuur 9 is dat www.forumstandardisatie.nl en (probeert) vervolgens het digitale (TLS) certificaat dat door de server wordt gepresenteerd op basis van de bijbehorende DANE TLSA-records in de DNS te verifiëren.)

```
TLSA-records found: 1
TLSA: 3 0 1 c6b0b0a9adb1530896e36919bc7a127257ed487d11b2b385903b3a809a4a9227

Connecting to IPv6 address: 2001:14a0:500:400::3673:2 port 443
TLSv1.2 handshake succeeded.
Cipher: TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
Peer Certificate chain:
0. Subject CN: www.forumstandaardisatie.nl
Issuer  CN: QuoVadis CSP - PKI Overheid CA - G2
1. Subject CN: QuoVadis CSP - PKI Overheid CA - G2
Issuer  CN: Staat der Nederlanden Organisatie CA - G2
2. Subject CN: Staat der Nederlanden Organisatie CA - G2
Issuer  CN: Staat der Nederlanden Root CA - G2
SAN dNSName: www.forumstandaardisatie.nl
SAN dNSName: forumstandaardisatie.nl
DANE TLSA 3 0 1 [c6b0b0a9adb1...] matched EE certificate at depth 0
Validated Certificate chain:
0. Subject CN: www.forumstandaardisatie.nl
Issuer  CN: QuoVadis CSP - PKI Overheid CA - G2
SAN dNSName: www.forumstandaardisatie.nl
SAN dNSName: forumstandaardisatie.nl

Connecting to IPv4 address: 80.246.186.158 port 443
TLSv1.2 handshake succeeded.
Cipher: TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
Peer Certificate chain:
0. Subject CN: www.forumstandaardisatie.nl
Issuer  CN: QuoVadis CSP - PKI Overheid CA - G2
1. Subject CN: QuoVadis CSP - PKI Overheid CA - G2
Issuer  CN: Staat der Nederlanden Organisatie CA - G2
2. Subject CN: Staat der Nederlanden Organisatie CA - G2
Issuer  CN: Staat der Nederlanden Root CA - G2
SAN dNSName: www.forumstandaardisatie.nl
SAN dNSName: forumstandaardisatie.nl
DANE TLSA 3 0 1 [c6b0b0a9adb1...] matched EE certificate at depth 0
Validated Certificate chain:
0.Subject CN: www.forumstandaardisatie.nl
Issuer  CN: QuoVadis CSP - PKI Overheid CA - G2
SAN dNSName: www.forumstandaardisatie.nl
SAN dNSName: forumstandaardisatie.nl

[0] Authentication succeeded for all (2) peers.
```

Figuur 9 TLSA-records voor www.forumstandaardisatie.nl

Het "Certificaat gebruik" veld

Dit veld geeft aan hoe de betreffende vingerafdruk/hashwaarde geïnterpreteerd moet worden.

Certificaat gebruik 0 en 1 verankeren een digitaal certificaat van respectievelijk een CA of een server in aanvulling op de traditionele validatie met behulp van de vertrouwensankers (trust anchors) meegeleverd in de clientapplicatie (bijvoorbeeld de browser). Daarmee wordt het probleem van de gekraakte CA gelokaliseerd (certificaat gebruik 0) of helemaal geneutraliseerd (certificaat gebruik 1). Bovendien worden op deze manier discrepanties tussen de twee vertrouwensketens gesignaleerd.

0. PKIX-TA: CA Beperking/Restrictie (Constraint): Certificaat gebruik 0 wordt gebruikt om een specifiek digitaal CA-certificaat, of de publieke

   sleutel van een dergelijke digitaal certificaat, in de vertrouwensketen te verankeren/specificeren. Hiermee wordt aangegeven welke CA kan worden vertrouwd om het digitaal (TLS) certificaat voor de betreffende dienst, dat door de server tijdens het opzetten van de TLS-versleutelde verbinding (Tunnel) wordt aangeleverd, te authenticeren. Kortom welke CA kan worden gebruikt om digitale certificaten voor een domein uit te geven.
   Dit digitaal certificaat gebruik wordt aangeduid als "CA beperking/restrictie" omdat het beperkt welke CA kan worden gebruikt om digitale (TLS) certificaten uit te geven voor een bepaalde dienst op een host. Het digitale (TLS) certificaat moet namelijk zijn uitgegeven door de opgegeven CA. De vingerafdruk/hashwaarde wordt gegenereerd uit het openbare CA-certificaat. Het gepresenteerde digitale (TLS) certificaat moet met succes de PKIX[38]

37 Het hulpmiddel dat hierbij is gebruikt is het 'Check a DANE TLS Service' van Shumon Huque https://www.huque.com/bin/danecheck

38 Zie RFC 5280 'PKIX Certificate and CRL Profile' (https://tools.ietf.org/html/rfc5280)

certificeringspad[39] validatie doorstaan en het CA-certificaat dat overeenkomt met het TLSA-record moet onderdeel zijn van het geldige certificeringspad. Dit certificaat gebruik is een aanvulling op de traditionele (offline) validatie.

1. PKIX-EE: Dienstcertificaat Beperking/Restrictie (Constraint):
   Certificaat gebruik 1 wordt gebruikt om een (eind) entiteit digitaal certificaat (dienstcertificaat), of de publieke sleutel van een dergelijke digitaal certificaat te verankeren/specificeren, dat moet worden vertrouwd voor deze dienst. Deze gegevens moeten overeenkomen met het (eind) entiteit digitaal certificaat dat door de server tijdens het opzetten van de TLS-versleutelde verbinding (Tunnel) wordt aangeleverd.
   Dit digitaal certificaat gebruik wordt aangeduid als "dienstcertificaat beperking/restrictie", omdat het een beperking oplegt welk (eind) entiteit digitaal certificaat kan worden gebruikt door een bepaalde dienst op een host. De vingerafdruk/hashwaarde wordt gegenereerd uit dit (eind) entiteit digitaal certificaat. Het gepresenteerde digitale certificaat moet met succes de PKIX certificeringspad validatie doorstaan en moet overeenkomen met het TLSA-record. Dit certificaat gebruik is een aanvulling op de traditionele (offline) validatie.

Certificaat gebruik 2 en 3 werken onafhankelijk van de traditionele TLS-validatie, en dat maakt ze geschikt voor zelfondertekende digitale certificaten. Bovendien kunnen op deze manier client applicaties bediend worden die helemaal geen vertrouwensankers (trust anchors) aan boord hebben. Dat laatste geldt bijvoorbeeld voor SMTP clients.

2. DANE-TA: Vertrouwensanker verklaring (Assertion)
   Certificaat gebruik 2 wordt gebruikt om een digitaal CA-certificaat of de publieke sleutel van het digitaal certificaat te specificeren. Deze gegevens moeten worden gebruikt als vertrouwensanker (trust anchor) bij het valideren van het (eind) entiteit digitaal certificaat dat door de server tijdens het opzetten van de TLS-versleutelde verbinding (Tunnel) wordt aangeleverd.
   Dit digitaal certificaat gebruik wordt aangeduid als "vertrouwensanker verklaring", omdat het de domeinnaambeheerder toestaat om een nieuw vertrouwensanker te specificeren. Bijvoorbeeld doordat het domein zijn eigen digitale certificaten uitgeeft onder zijn eigen CA en die naar verwachting niet tot de verzameling van vertrouwensankers (trust anchor) behoort in de client applicaties van de eindgebruikers.
   Het gepresenteerde digitale certificaat moet met succes de PKIX certificeringspad validatie doorstaan, waarbij ieder digitaal certificaat dat overeenkomt met het TLSA-record wordt gezien als een vertrouwensanker tijdens deze certificeringspad validatie.

   Het TLSA RR wordt door de clientapplicatie (bijvoorbeeld browser zoals Mozilla Firefox, Google Chrome en Microsoft Internet Explorer) ontvangen als gevolg van DNSSEC validatie. De clientapplicatie (bijvoorbeeld browser) moet tijdens het uitvoeren van de digitale certificaat validatie zekerstellen dat de CA van het gepresenteerde digitale certificaat hetzelfde is als die van de TLSA payload. Hier vindt geen vertrouwensketen verificatie plaats.

3. DANE-EE: Domein uitgegeven certificaat:
   Certificaat gebruik 3 wordt gebruikt om een digitaal certificaat of de publieke sleutel van het digitaal certificaat te specificeren. Deze gegevens moeten overeenkomen met het (eind) entiteit digitaal certificaat dat door de server tijdens het opzetten van de TLS-versleutelde verbinding (Tunnel) wordt aangeleverd. De clientapplicatie authenticeerd de server als het gepresenteerde digitaal certificaat overeenkomt met de TLSA payload.
   Dit digitale certificaat gebruik wordt aangeduid als "domein uitgegeven certificaat", omdat het de domeinnaambeheerder toestaat om digitale certificaten voor een domein uit te geven, zonder tussenkomst van een derde partij CA. Een vingerafdruk/hashwaarde van het digitaal certificaat wordt toegevoegd in de zone van het domein als gegevensveld waarmee het digitaal (TLS) certificaat moet worden geassocieerd van het TLSA RR.
   Het beoogde digitale certificaat moet overeenkomen met het TLSA-record. Het verschil tussen certificaat gebruik 1 en certificaat gebruik 3 is dat certificaat gebruik 1 vereist dat het digitale certificaat met succes de PKIX validatie doorstaat, maar PKIX validatie wordt niet getest bij certificaat gebruik 3.

Het "Keuze" veld

Het "keuze" veld specificeert welk deel van het digitale certificaat dat door de server wordt aangeleverd wordt vergeleken met de overeenkomstige gegevens uit het TLSA-record. De keuzemogelijkheden zijn:
0 – Volledig certificaat: De binaire structuur van het certificaat zoals gedefinieerd in RFC 5280.[40]
1 – SubjectPublicKeyInfo (Bevat de publiek sleutel van het subject): DER-gecodeerde binair structuur zoals gedefinieerd in RFC 5280.

Het "Bijpassend Type" veld

Het zogenaamde "bijpassend type" geeft aan hoe de certificaatkoppeling wordt gepresenteerd. De keuzemogelijkheden zijn:
0 - Exacte overeenkomst met de geselecteerde content
1 - SHA-256 hashwaarde van geselecteerde content.[41]
2 - SHA-512 hashwaarde van geselecteerde content.

Als het bijpassend type in het TLSA-record een hashwaarde betreft, wordt geadviseerd om zoveel mogelijk hetzelfde hashalgoritme te gebruiken als dat werd gebruikt bij het genereren van de digitale handtekening in het digitale certificaat. Dit vergroot de toepasbaarheid en dan met name voor client applicaties die maar een beperkt aantal hashalgoritmen ondersteunen.

39 Certificaatketen op basis van X.509.

40 Zie https://tools.ietf.org/html/rfc5280
41 Voor zowel SHA 256 (type 1) als 512 (type 2) geldt dat dit op basis van RFC 6234 is (https://tools.ietf.org/html/rfc6234)

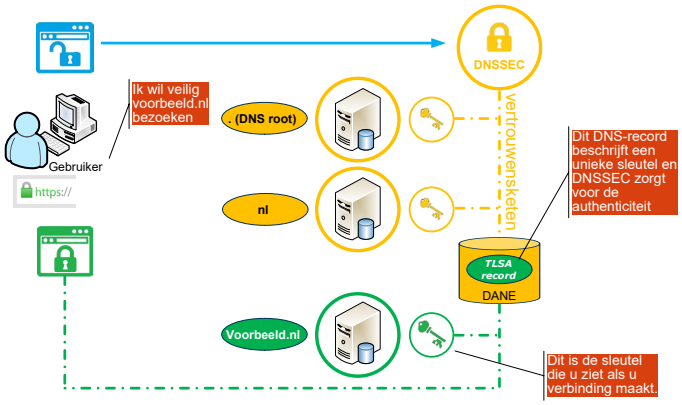
Het advies is om voor elke (e-mail of web) server twee TLSA-records aan te maken. Het ene record, het '2 1 1'-record, verwijst naar de CA. Het andere record, het '3 1 1'-record, verwijst naar

het digitaal certificaat zelf. Op die manier leiden kleine fouten in de configuratie niet meteen tot onbeschikbaarheid van uw e-mailvoorziening.[42]
Gebruik een TLSA hulpmiddel (tool) om eenvoudig TLSA-records te genereren. Bijvoorbeeld:

- Er zijn verschillende command line tools beschikbaar die hiervoor kunnen worden gebruikt, bijvoorbeeld:
- hash-slinger[43] van Paul Wouters.
- ldns-dane[44], onderdeel van de ldns library van NLnet Labs
- swede[45] van Pieter Lexis.
- Wie liever met een web gebaseerd online tool werkt kan gebruik maken van:
- DNS TLSA resource record generator van Shumon Huque.[46]
- TLSA-record Generator van SSL-Tools.[47]

TLSA-record validatie

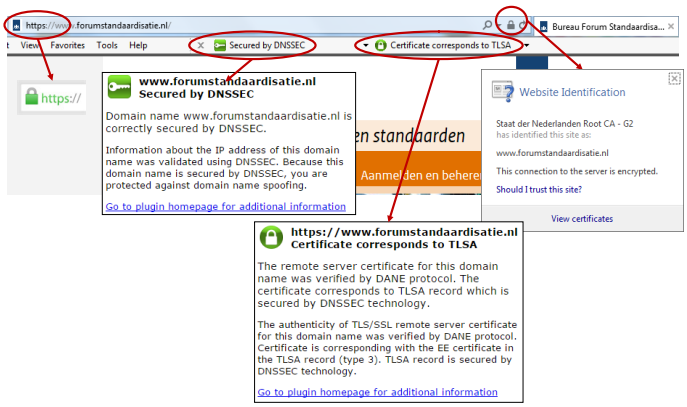
Het nadeel van DANE is dat de meeste client applicaties op dit moment nog niet standaard het TLSA-record kunnen verifiëren, maar hiervoor afhankelijk zijn van externe add-ons/ plug-ins. Als oplossing zou de gemeente ervoor kunnen kiezen om het eigen digitale certificaat door een vertrouwde CA, die wel in de clientapplicatie is opgenomen, te laten ondertekenen.



Figuur 10 Beveiliging voor TLS met DANE

De DNSSEC / TLSA Validator is een web browser add-on die het mogelijk maakt om het bestaan en de geldigheid van DNS-records die met DNSSEC zijn ondertekend te controleren. Met deze add-on worden de DNSSEC- en TLSA-records gerelateerd aan een domeinnaam gecontroleerd. Als een geldige DNSSEC vertrouwensketen voor het betreffende domein is gevonden zal de plug-in ook het bestaan en de geldigheid van TLSA-records controleren. De resultaten van DNSSEC en TLSA validatie worden gepresenteerd met behulp van verschillende pictogrammen (zie Figuur 11). Extra toelichtende teksten worden voor Mozilla Firefox en Google Chrome weergegeven op de adresbalk

of voor Microsoft Internet Explorer in een aparte toolbar. Als u op het weergegeven pictogram klikt toont meer gedetailleerde informatie over de toestand van de veiligheid.[48]



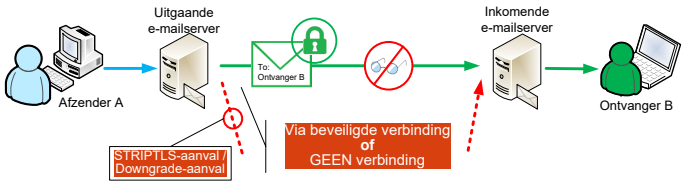
Figuur 11 DNSSEC en TLSA validatie in de gebruikers applicatie (browser).

Achtergrondinformatie met betrekking tot e-mail

Voor het uitwisselen van e-mailberichten wordt gebruik gemaakt van het standaard (de facto) protocol Simpel Mail Transport Protocol (SMTP)[49]. Dit SMTP-protocol is een relatief simpel, tekst gebaseerd protocol, dat geen betrouwbare voorzieningen bevat om na te gaan of de afzender echt is wie hij beweert te zijn. Deze beperking biedt derden de mogelijkheid om e-mailberichten te versturen namens andere e-mailadressen. Zonder extra maatregelen is er geen enkele zekerheid of een e-mailbericht wel echt afkomstig is van de organisatie namens welke het e-mailbericht verstuurd wordt.

WAT LEVERT DE COMBINATIE STARTTLS EN DANE MIJN GEMEENTE OP?

STARTTLS in combinatie met DANE maakt het mogelijk om een beveiligde verbinding voor e-mailverkeer tot stand te brengen en gaat het afluisteren of manipuleren van e-mailverkeer tegen. De complementaire standaard DANE maakt het voor de eigenaar van een domein mogelijk om via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline digitale certificaten aan te reiken als extra verificatiemiddel. Hierdoor kan realtime een controle worden gedaan op de authenticiteit van de e-mailserver en of de server-to-server verbinding legitiem is en niet wordt gemanipuleerd. De afzender weet hierdoor dat het e-mailbericht daadwerkelijk via een versleutelde verbinding is verstuurd naar een e-mailserver van de ontvangende partij, zonder dat deze onderweg is onderschept of gemanipuleerd.



Figuur 12 E-mailverkeer met gebruik van TLS, STARTTLS en DANE

Wanneer zowel de verzendende als de ontvangende partij DANE toepassen wordt een verbinding pas tot stand gebracht wanneer het DNS-record van de ontvangende partij gecontroleerd is door de verzendende partij. Gebruikers van DANE en STARTTLS moeten, conform Request for Comments (RFC) 7672[50], de verbinding verbreken wanneer er geen beveiligde verbinding via STARTTLS opgezet kan worden maar deze wel aanwezig is volgens het DNS-record. Hiermee worden STRIPTLS-aanvallen voorkomen (zie Figuur 12).

42 Deze methode is gebaseerd op de analyse uit https://www.ietf.org/mail-archive/web/uta/current/msg01498.html
43 Zie https://github.com/letoams/hash-slinger.
44 Zie https://www.nlnetlabs.nl/projects/ldns/
45 Zie https://github.com/pieterlexis/swede
46 Zie https://www.huque.com/bin/gen_tlsa
47 Zie https://ssl-tools.net/tlsa-generator

48 Op de website van DNSSEC/TLSA Validator worden de mogelijke instellingen en uitleg van de pictogrammen weergegeven. https://www.dnssec-validator.cz/pages/documentation.html
49 Zie: https://tools.ietf.org/html/rfc5321
50 https://tools.ietf.org/html/rfc7672

STAPPENPLAN

Om STARTTLS en DANE op **inkomend** e-mailverkeer te implementeren:

1. Inventariseer op welke e-mailservers uw gemeente e-mailberichten ontvangt.
   - Neem de e-mailservers op die e-mailberichten ontvangen van andere externe e-mailservers. Dat kunnen e-mailservers zijn die de gemeente niet zelf beheert, zoals e-mailservers van een spamfilterdienst.
   - Neem elke e-mailserver op die in de Mail eXchange (MX)-records[51] van de gemeentelijke domeinnamen staan.
   - U kunt ook interne e-mailstromen beveiligen met STARTTLS en DANE. U kunt deze e-mailstromen echter ook met alternatieve maatregelen beveiligen, zoals het pinnen van een publieke sleutel.[52] Mogelijk gebruikt uw gemeente zulke maatregelen al.
2. Kies of u STARTTLS aanbiedt met behulp van een openbare CA of een eigen CA.
   - Gebruik een openbare CA als u niet de kennis of middelen heeft om een eigen CA op te zetten en te beheren.
   - Zorg dat elke e-mailserver zijn eigen digitaal certificaat heeft. Zet de Fully Qualified Domain Name (FQDN)[53] van de e-mailserver in het digitaal certificaat als Subject Alternative Name.
3. Schakel STARTTLS in op elke inkomende gemeentelijke e-mailserver.
4. Schakel op elke e-mailserver op uw lijst STARTTLS in.
   - Stel STARTTLS in op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security van het NCSC.[54] Gebruik het digitaal certificaat dat voor deze e-mailserver is aangemaakt. Stel de e-mailserver zo in dat de hele keten van digitale certificaten tot en met de CA wordt meestuurt.
5. Publiceer voor elke inkomende gemeentelijke e-mailservers de TLSA-records in de DNS-zone van deze e-mailserver.
   - Handelt bijvoorbeeld de e-mailserver mail.voorbeeld.org de e-mailberichten af van het domein voorbeeld.nl, dan plaatst u de TLSA-records in de DNS-zone voorbeeld.org.
   - Zorg dat DNSSEC is ingeschakeld, zowel op de DNS-zone van het e-maildomein als op de DNS-zone waarin de TLSA-records staan.
   - Let op: Zonder DNSSEC weet de afzender niet met zekerheid tegen welk MX-domeinnaam het digitaal certificaat dient te worden gevalideerd.[55]
6. Controleer regelmatig of uw instellingen kloppen en werken.
   - Bijvoorbeeld: kloppen en werken de DNSSEC-instellingen, is de e-mailserver via STARTTLS bereikbaar.
   - Gebruik daarvoor de hulpmiddelen zoals beschreven in het onderdeel 'Hulpmiddelen'.
   - Sommige firewalls zijn standaard zo ingesteld dat deze STARTTLS strippen van alle inkomende e-mailstromen. Als uw e-mailserver niet bereikbaar is via STARTTLS, pas dan de netwerkconfiguratie aan om de e-mailserver wel via STARTTLS bereikbaar te maken.
   - Als u DANE en STARTTLS gebruikt voor e-mailberichten, hangt de beschikbaarheid van uw e-mailvoorziening af van DNSSEC.
7. Beschrijf het beheerproces rondom digitale certificaten. Wie is verantwoordelijk voor het aanvragen en intrekken van certificaten? Maak een back-up van al uw digitale certificaten en sla die op een veilige offline plek op.[56]
8. Vervang het digitaal certificaat van een e-mailserver als het verlopen is, of als u het vermoeden heeft dat een kwaadwillende de privésleutel heeft weten te bemachtigen of is gecompromitteerd.
   - Genereer eerst het nieuwe digitale certificaat en laat het ondertekenen door uw eigen gemeentelijke of openbare CA. Stel het in op de e-mailserver. Wijzig daarna het TLSA-record met type '3 1 1' van de e-mailserver zodat het verwijst naar het nieuwe certificaat.
   - Bij een nieuw certificaat van een andere CA dient nog een extra stap doorlopen te worden. Vervang eerst het TLSA-record met type '2 1 1' door een TLSA-record met type '2 1 1' dat verwijst naar de nieuwe CA. Wacht vervolgens tot de 'time-to-live' (TTL)[57] van de TLSA-records verlopen is. Het oude '2 1 1'-record komt dan niet meer in caches van DNS-servers voor. Voer vervolgens de procedure uit van het vorige opsommingsteken uit: genereer een nieuw certificaat, laat het ondertekenen door de nieuwe CA, stel het in op de e-mailserver en vervang het '3 1 1'-record.
   - Roll-over: Net als voor HTTPS is het ook voor e-mail van belang om niet te vergeten het TLSA-record opnieuw aan te maken als het digitaal servercertificaat wordt vervangen. Ook hiervoor moet een complete roll-over worden uitgevoerd: Eerst moet het nieuwe TLSA-record worden toegevoegd. Nadat de nieuwe Resource Record Set (RRset)[58] overal bekend is, kan het digitale servercertificaat worden vervangen. En pas daarna kan het oude TLSA-record worden weggehaald.

51 Een MX-record bevat de naam van de e-mailserver die het e-mailverkeer voor het betreffende domein afhandelt. Een domein kan meerdere MX-records hebben met een verschillende prioriteit waardoor het mogelijk is om bijvoorbeeld een back-up e-mailserver aan te geven als de e-mailserver met de hogere prioriteit niet bereikbaar blijkt. De naam die in het MX-record wordt gevonden wordt via DNS weer vertaald naar een IP-adres

52 HTTP Public Key Pinning (HPKP), soms ten onrechte certificaat pinning genoemd, is een beveiligingsmechanisme waarmee HTTPS-websites nabootsing door aanvallers die gebruik maken van verkeerd uitgegeven of anderszins frauduleuze digitale certificaten kunnen tegengaan. Bijvoorbeeld, kwaadwillenden zouden een CA kunnen compromitteren, en daarna 'valse' digitale certificaten kunnen uitgeven voor websites. Om dit risico tegen te gaan, levert de HTTPS webserver een lijst van "vastgepinde" hashwaarden van publieke sleutels; op de volgende verbindingen verwacht de client applicatie dat de server één of meer van deze publieke sleutels gebruikt in zijn digitale certificaat vertrouwensketen. (https://tools.ietf.org/html/rfc7469)

53 Een fully qualified domain name (FQDN). Als de gemeente bijvoorbeeld een server met hostname 'mijnserver' heeft en domeinaam'mijndomeinnaam.nl', dan wordt de FQDN 'mijnserver.mijndomeinnaam.nl'

54 Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

55 Zie: https://blog.filippo.io/the-sad-state-of-smtp-encryption/

56 Zie hiervoor ook de factsheet 'Veilig beheer van digitale certificaten' van het NCSC: https://www.ncsc.nl/actueel/factsheets/factsheet-veilig-beheer-van-digitale-certificaten.html.

57 De TTL van de domeinnaam bepaalt hoe lang een resolver een vraag voor een domeinnaam cacht.

58 Bevat alle records van een bepaald type voor een bepaald domein. Bijvoorbeeld zou een complete RRset voor 'mijnserver.mijndomein.nl' voor de 'A' set van gegevens, alle A (IPv4) records voor 'mijnserver.mijndomein.nl' bevatten.

Om STARTTLS en DANE op **uitgaand** e-mailverkeer te implementeren:

Zoals door het Forum Standaardisatie aangegeven is de implementatie van STARTTLS in combinatie met DANE voor uitgaande e-mailservers ingewikkelder en vraagt meer inzet in tijd en middelen.[59]

1. Inventariseer alle e-mailservers waarmee uw gemeente e-mail verstuurt.
   - Neem de e-mailservers op die e-mailberichten versturen aan andere externe e-mailservers.
   - Interne e-mailstromen kunnen ook worden beveiligd met STARTTLS en DANE. Deze e-mailstromen kunnen echter ook met alternatieve maatregelen beveiligd worden, zoals het pinnen van een digitaal certificaat.
2. Ga van elke geïnventariseerde e-mailserver na of de geïmplementeerde e-mailserversoftware DANE en STARTTLS ondersteunt voor uitgaande e-mailberichten. Raadpleeg hiervoor de documentatie van uw e-mailserver.

Voer stap 3 uit als uw e-mailserver DANE en STARTTLS ondersteunt en voer stap 4 uit als uw e-mailserver geen DANE maar wel STARTTLS ondersteunt.

3. Schakel DANE en STARTTLS in op elke uitgaande e-mailserver van uw gemeente.
   - Deze e-mailservers moet daarvoor wel DNSSEC-validatie uit kunnen voeren.
   - Stel STARTTLS in op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security van het NCSC. Gebruik het digitaal certificaat dat voor deze e-mailserver is aangemaakt. Stel de e-mailserver zo in dat de hele keten van digitale certificaten tot en met de CA wordt meestuurt.
   - Gebruik de optie om DANE-validatie uit te voeren alleen als er TLSA-records beschikbaar zijn. Deze optie heet ook wel 'opportunistische DANE-validatie'. Zorg dat de e-mailserver beschikt over een betrouwbare verbinding naar een DNSSEC-validerende recursive DNS-nameserver. Bijvoorbeeld door er lokaal op de e-mailserver een te draaien.
4. Installeer en configureer een aparte e-mailserver in als relay voor deze e-mailserver.
   - Gebruik op deze nieuwe e-mailserver software die wel STARTTLS en DANE ondersteunt.
   - Gebruik het pinnen van een digitaal certificaat om de verbinding tussen de bestaande en de nieuwe e-mailserver te beveiligen.
   - Schakel ondersteuning voor STARTTLS en DANE in op de nieuwe e-mailserver, volgens punt 3.
5. Publiceer voor elke uitgaande gemeentelijke e-mailservers de TLSA-records in de DNS-zone van deze e-mailserver.
6. Controleer regelmatig of uw instellingen kloppen en werken.
   - Bijvoorbeeld: kloppen en werken de DNSSEC-instellingen, is de e-mailserver via STARTTLS bereikbaar.
   - Gebruik daarvoor de hulpmiddelen zoals beschreven in het onderdeel 'Hulpmiddelen'.
   - Als u DANE en STARTTLS gebruikt voor e-mailberichten, hangt de beschikbaarheid van uw e-mailvoorziening af van DNSSEC.
7. Vervang het digitaal certificaat van een e-mailserver als het verlopen is, of als u het vermoeden heeft dat een kwaadwillende de privésleutel heeft weten te bemachtigen of is gecompromitteerd.
   - Genereer eerst het nieuwe digitale certificaat en laat het ondertekenen door uw eigen gemeentelijke of openbare CA. Stel het in op de e-mailserver. Wijzig daarna het TLSA-record met type '3 1 1' van de e-mailserver zodat het verwijst naar het nieuwe certificaat.
   - Roll-over: Net als voor HTTPS is het ook voor e-mail van belang om niet te vergeten het TLSA-record opnieuw aan te maken als het digitaal servercertificaat wordt vervangen. Ook hiervoor moet een complete roll-over worden uitgevoerd: Eerst moet het nieuwe TLSA-record worden toegevoegd. Nadat de nieuwe Resource Record Set (RRset)[60] overal bekend is, kan het digitale servercertificaat worden vervangen. En pas daarna kan het oude TLSA-record worden weggehaald.

Hulpmiddelen

Hulpmiddelen waarmee de DANE configuratie kan worden gecontroleerd zijn onder andere:

- Website en e-mail zelftest via Internet.nl[61]
- DANE TLSA-record zelftest via SIDNLabs.nl[62]
- DANE SMTP-validator van sys4[63]

59 https://www.forumstandaardisatie.nl/standaard/starttls-en-dane

60 Bevat alle records van een bepaald type voor een bepaald domein. Bijvoorbeeld zou een complete RRset voor 'mijnserver.mijndomein.nl' voor de 'A' set van gegevens, alle A (IPv4) records voor 'mijnserver.mijndomein.nl' bevatten

61 Zie: https://internet.nl/

62 Zie: https://check.sidnlabs.nl/dane/

63 Zie: https://dane.sys4.de/

ADVIEZEN IBD MET BETREKKING TOT STARTTLS EN DANE

De IBD geeft het advies om:

- STARTTLS en DANE in te schakelen voor al het inkomende e-mailverkeer van uw gemeente. Op die manier kan elke andere organisatie betrouwbaar communiceren met uw e-mailservers.
- STARTTLS en DANE in te schakelen voor al het uitgaande e-mailverkeer van uw gemeente. Op het moment dat andere organisaties ook STARTTLS en DANE hebben ingeschakeld voor hun inkomende e-mailverkeer, kan uw gemeente betrouwbaar communiceren met de organisaties die STARTTLS en DANE toepassen voor hun e-mailservers.
- Voor het configureren van STARTTLS en DANE de factsheet 'Beveilig verbindingen van mailservers' van het NCSC te volgen.
- Ervoor te zorgen dat uw gemeente beschikt over de benodigde kennis en tooling voor het aanmaken van TLSA-records. Als uw gemeente niet over de benodigde kennis en/of tooling beschikt, kan uw gemeente kiezen voor een kundige externe implementatiebegeleider of opdracht geven aan uw hostingpartij.
- Voor elke e-mailserver twee TLSA-records aan te maken. Het ene record verwijst naar de certificaatautoriteit (CA). Het andere record verwijst naar het digitale certificaat zelf. Op die manier leiden (kleine) fouten in de configuratie niet meteen tot onbeschikbaarheid van uw e-mailvoorziening.
- DNSSEC te gebruiken, zowel op de DNS-zone van het e-maildomein als op de DNS-zone waarin de TLSA-records staan. DNSSEC zorgt ervoor dat uitgaande e-mailservers de authenticiteit van informatie in TLSA-records kunnen controleren. Alleen met DNSSEC heeft het publiceren van TLSA-records effect. Voor meer achtergrondinformatie van DNSSEC de factsheet 'DNSSEC: Voorkom domeinnaamfraude' van de IBD te lezen. Controleer regelmatig of uw instellingen kloppen en werken. Gebruik daarvoor de hulpmiddelen zoals beschreven in het onderdeel 'Hulpmiddelen'. Controleer ook of uw DNSSEC-instellingen kloppen en werken. Als u (STARTTLS en) DANE gebruikt voor e-mail, hangt de beschikbaarheid van uw e-mailvoorziening af van DNSSEC.
- Beschrijf het beheerproces rondom digitale certificaten en maak een back-up van al uw digitale certificaten en sla die op een veilige offline plek op.
- Vervang het digitale certificaat van een e-mailserver als het verlopen is, of als u het vermoeden heeft dat een kwaadwillende de privé sleutel heeft weten te bemachtigen. Genereer eerst het nieuwe certificaat en laat het ondertekenen door uw eigen of de openbare CA. Stel het in op de e-mailserver. Wijzig daarna het TLSA-record van de e-mailserver zodat het verwijst naar het nieuwe certificaat.
- Maak een lijst van alle e-mailservers waarmee uw gemeente e-mailbericht verstuurt. Neem de servers op die e-mail versturen aan andere externe e-mailservers. U kunt ook interne e-mailstromen beveiligen met (STARTTLS en) DANE. Ga van elke e-mailserver op uw lijst na of de gebruikte e-mailserversoftware (STARTTLS en) DANE ondersteunt voor uitgaande e-mailberichten. Raadpleeg hiervoor de documentatie van uw e-mailserver.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.