1.1 Wat is het

DKIM staat voor Domain Keys Identified Mail. Het is een techniek die de veiligheid van verstuurde e-mails vergroot. Van nature is het gebruik van e-mail onveilig. Internet criminelen zetten daarom vaak e-mail in voor frauduleuze acties, zoals het versturen van phishing (lees hier meer informatie over phishing). Met de inzet van DKIM kun je dit in belangrijke mate voorkomen.
DKIM is een standaard om ervoor te zorgen dat je zeker weet dat een e-mail bericht afkomstig is van het domein waarvan het zegt afkomstig te zijn (@klantnaam.nl vaak dus) en of het e-mail bericht tussen het versturen en ontvangen niet veranderd is. Samen met twee andere standaarden (SPF en DMARC, zie bijlage), zorgt dit voor veilig e-mail gebruik.

1.2 Voor wie is het nuttig

DKIM is voor alle klanten die vanuit Livits e-mail versturen (denk aan de nieuwsbrieven module) relevant.

Let op: Het is vaak zo dat er meerdere externe organisaties zijn die voor een ledenorganisatie e-mail versturen. Voor een goede e-mail veiligheid is het van belang dat alle e-mail stromen in beeld zijn en deze allemaal zo veilig mogelijk worden gemaakt. DKIM moet door elke partij worden geïmplementeerd, die e-mail namens de betreffende ledenorganisatie verstuurd. Door DKIM af te nemen bij CCI doe je dat uitsluitend voor de e-mailstroom vanuit Livits.

1.3 Wat is het voordeel

Met de implementatie van DKIM geef je meer zekerheid aan de ontvangers van e-mail vanuit Livits. Dit maakt dat internetfraudeurs met phishing mails minder kans krijgen bij de bij ledenorganisaties aangesloten partijen.

Let op: Voor echt veilig e-mail gebruik, is het nodig dat naast DKIM ook de twee standaarden (SPF en DMARC) zoals toegelicht in de bijlage worden geïmplementeerd. Voor DKIM geldt dat wij dit moeten doen (in afstemming met de betreffende ledenorganisatie). Voor de andere twee standaarden geldt dat dit vooral door de betreffende ledenorganisatie moet worden uitgevoegd (op onderdelen in afstemming met ons).

1.4 Wat doen wij voor jullie

DKIM is iets dat wij in moeten stellen in onze e-mail server. Een DKIM record in de DNS van de ledenorganisatie geeft aan dat DKIM gebruikt wordt. Dit moet de DNS beheerder bij de ledenorganisatie toevoegen, dit wordt door ons afgestemd. Wij hebben DKIM al operationeel bij meerdere Livits klanten.
Om DKIM goed te laten werken is aan onze kant configuratie van Livits noodzakelijk. Hiervoor schaffen wij software aan die de DKIM implementatie mogelijk maakt. Deze wordt op de mailserver waarmee Livits e-mail stuurt geïnstalleerd.

Het implementeren van DKIM moeten we inplannen. Na opdracht heeft dit een doorlooptijd van 2 tot 4 weken.

1.5 Meer informatie

De overheid heeft het gebruik van DKIM en SPF als een verplichte standaard verklaard voor overheidsdiensten. Dit geeft ook wel aan hoe belangrijk het is. Wil je meer weten over DKIM of de andere standaarden, check dan de onderstaande sites:

- https://www.forumstandaardisatie.nl/open-standaarden/dkim
- https://nl.internet.nl/faqs/mailauth/

Een simpele veiligheidstest op bijvoorbeeld www.Internet.nl laat zien hoe veilig de website of het e-mail adres van een omgeving is. Daar wordt ook gecontroleerd op de aanwezigheid van DKIM en de andere e-mail veiligheidsstandaarden.

Let op: Als een check aangeeft dat DKIM geïmplementeerd is, voor een domein, wil dit niet zeggen dat dit ook bij Livits is uitgevoerd. Neem contact met ons op als je hierover vragen hebt.

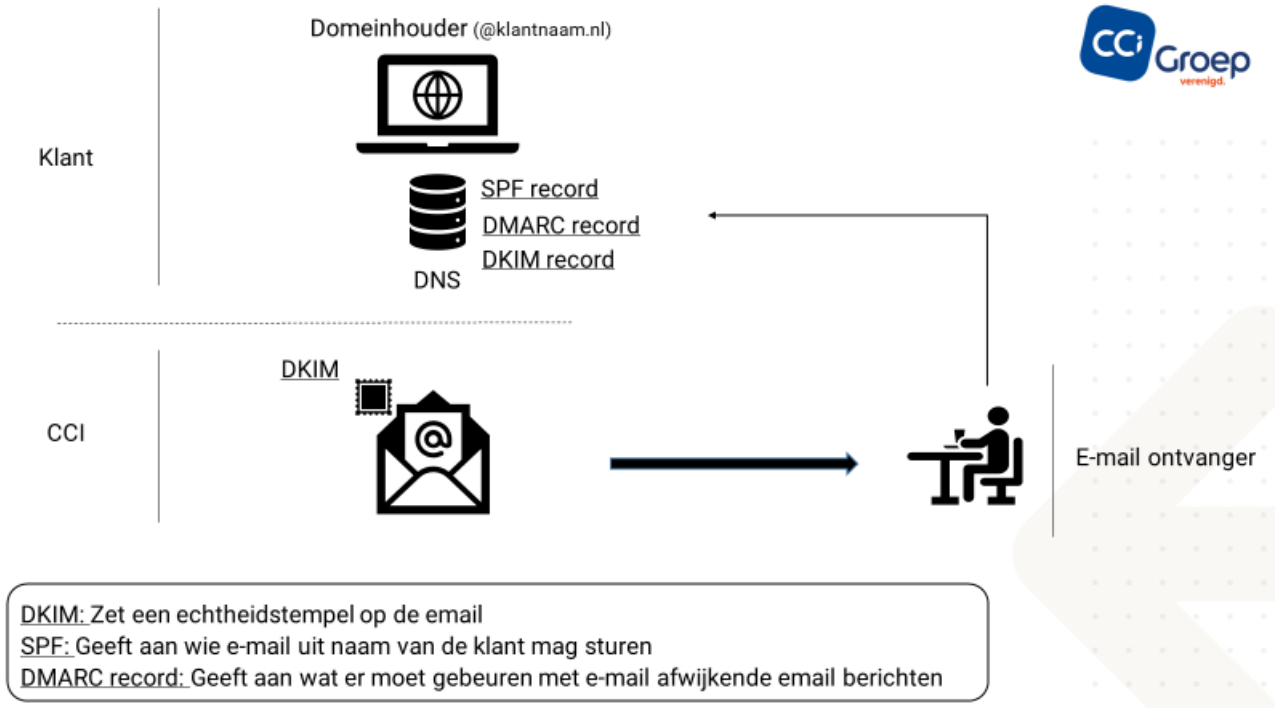
1.6 De andere e-mail beveiligingsstandaarden

Naast DKIM zijn er nog twee andere standaarden die de e-mail veiligheid verhogen:

- SPF: Dit is een record in de DNS van de ledenorganisatie (de domeinhouder) waarin staat vanuit welke IP adressen e-mail gestuurd mag worden uit naam van deze organisatie. Dit is hoofdzakelijk niet iets wat CCI kan doen, het meeste werk ligt bij de ledenorganisatie. CCI moet het IP adres van Livits aangeven, zodat dat door een ledenorganisatie in het SPF record kan worden opgenomen. Wel moet CCI ook wat in de eigen DNS configureren.
- DMARC: Is de standaard waarmee ontvangende e-mail servers bepalen wat er moet gebeuren. Dit werkt dus op basis van DKIM en SPF en dus met name de DNS instellingen bij de ledenorganisatie. Als deze allemaal goed zijn ingesteld, vertelt de DMARC policy wat er vervolgens voor dat afwijkende e-mail moet gebeuren (niet accepteren, als SPAM accepteren, niets mee doen en gewoon afleveren).

1.7 Schematisch

Hieronder wordt schematisch en versimpeld weergegeven hoe de verschillende standaarden samenwerken.



Wanneer een e-mail bericht dus ontvangen wordt door een e-mail programma, vinden een aantal controles plaats. Het e-mail programma kijkt van welk domein de mail afkomstig is (@klantnaam.nl). Dan wordt de DNS van dit domein geraadpleegd. Er wordt gekeken of er vanuit het IP adres waar de e-mail vandaan komt ook e-mail vanuit dit domein mag worden gestuurd (SPF check). Ook wordt gekeken of DKIM is geïmplementeerd (DKIM record). Als dat het geval is, wordt gekeken of de e-mail een DKIM stempel bevat. Beide checks zijn DMARC checks, en als hier een afwijking wordt geconstateerd wordt in het DMARC record van de DNS gekeken wat er moet gebeuren met afwijkende e=mail berichten (e-mail niet accepteren, e-mail als SPAM bestempelen of gewoon afleveren).