Substructure

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

# EMAILBEVEILIGING

Voldoet de beveiliging van uw emailverkeer aan de laatste beveiligingsstandaarden?

Wij verzorgen graag vrijblijvend een gratis scan van de beveiliging van uw infrastructuur waarmee u mail verstuurt.

Hiervoor kunt u contact opnemen via het emailadres scan@substructure.nl onder vermelding van uw domeinnaam of via telefoonnummer +31 6 136 17 631.

De gratis scan verrichten wij op de volgende onderdelen:

- Email Authenticatie;
- Versleuteling tussen mailservers.

Meer informatie over deze onderdelen vindt u later terug in deze brochure. U treft in deze brochure ook informatie aan over versleuteling van individuele emailberichten. Aan deze brochure is een begrippenlijst toegevoegd.

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

## EMAIL AUTHENTICATIE (DMARC, SPF, DKIM)

Voorkom dat een ander mailt uit naam van uw organisatie en behoed u voor de reputatieschade die een phishingaanval u kan bezorgen. Als organisatie zit u er niet op te wachten om berichtgevingen te moeten publiceren over emailberichten die zogenaamd uit naam van uw bedrijf zijn verstuurd.

Substructure heeft veel expertise met het inrichten van standaarden waarmee phishingmails kunnen worden gereduceerd. Wij helpen u hiermee graag verder.

**Hoe doen we dit?**

Met behulp van de DMARC standaard (in onze brochure DMARC leest u over deze standaard) en de authenticatiemethodes SPF en DKIM.

DMARC is een standaard die door alle grote technologie bedrijven zoals Google, Microsoft, Yahoo, Facebook en LinkedIn wordt ondersteund. In Nederland is XS4ALL als eerste begonnen om inkomende emailberichten aan de hand van deze standaard te controleren. Elke dag komen er bedrijven bij die de DMARC standaard inzetten om phishing te voorkomen.

Met DMARC kunt u als verzender via DNS een beleid publiceren. DMARC hanteert onderstaande beleidsinstellingen:

- none = niets doen;
- quarantine = naar spambox;
- reject = weigeren.

Als de ontvanger een emailbericht namens uw organisatie ontvangt zal hij deze met SPF en DKIM authentiseren. Indien uw emailbericht niet door de authenticatie heen komt zal de ontvanger het door u gepubliceerde beleid op het emailbericht toepassen. De ontvanger zal over alle emailberichten die hij namens uw organisatie heeft ontvangen via een standaard rapportage melden hoe deze zijn afgehandeld. Indien het beleid quarantine of reject wordt toegepast dan kan de ontvanger naast de standaard rapportage u ook direct een fout (failure) rapportage toesturen. De ontvanger stuurt de rapportages naar het door u ingesteld emailadres. De rapportages zijn technisch van aard en voor een leek niet te lezen. Onze onlinedienst MailReport maakt deze rapportages voor u inzichtelijk en begrijpelijk.

Indien gewenst kunt u als ontvanger ook de emailberichten vanuit andere organisaties controleren en hierover terug rapporteren. Hiermee helpt u deze organisaties hun emailverkeer in kaart te brengen met het uiteindelijke doel de niet legitieme verkeersstromen van deze organisaties op hun verzoek te kunnen verwijderen. De functionaliteit van het controleren en terug rapporteren kan op uw mailserver(s) worden aangezet / toegevoegd.

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

**MailReport**

MailReport is een online dienst die door Substructure is ontwikkeld. U kunt naar deze dienst uw rapportages laten opsturen. MailReport verwerkt deze rapportages en presenteert deze overzichtelijk via een zelf in te delen dashboard. Zo krijgt u een goed beeld van de legitieme en niet legitieme emailberichten die namens uw organisatie zijn verstuurd. MailReport geeft u inzicht in eventuele configuratiefouten van de mailserver(s) en authenticatiemechanismes. MailReport helpt u de benodigde configuratie te controleren en op orde te krijgen.

MailReport biedt de ondersteuning die u nodig heeft voor het dagelijks gebruik en maakt phishingaanvallen zichtbaar.

**Wat levert het op?**

Na volledige invoering biedt DMARC in combinatie met MailReport de onderstaande voordelen. DMARC en MailReport:

- verwijdert exacte domein phishing;
- verhoogt uw domein reputatie zodat meer emailberichten aankomen en niet verdwijnen in de spambox van uw ontvangers;
- geven u inzicht in het legitieme als ook niet legitieme emailverkeer op de door u geregistreerde domeinen;
- geven u inzicht in mail verzendende infrastructuur inclusief van leveranciers die ook namens u emailberichten versturen;
- verhoogt uw digitale imago en security reputatie. De reputatie wordt zichtbaar als zijnde reporter van rapportages (check op policy inkomende emailberichten) en gepubliceerd beleid via DNS;

Tevens:

- behoedt het u voor toekomstige aansprakelijkheid en de hieruit voortvloeiende claims (Wet Persoonsgegevens en Datalekken);
- bent u compliant met de pas toe of leg uit lijst (specifiek voor overheidsinstanties);
- bent u compliant met de BIR/BIG/BIWA (specifiek voor overheidsinstanties).

**Wat is de conclusie?**

- Het genereren en controleren op DKIM heeft invloed op de resource belasting van uw mailserver;

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

**Wat kost het?**

Voor de éénmalige ondersteuning om DMARC , SPF en DKIM op orde te krijgen bieden wij u een vrijblijvende offerte aan op basis van fixed fee. De hoogte van de offerte is afhankelijk van de grootte en de complexiteit van uw organisatie. U kunt ook kiezen voor een aanbieding op basis van nacalculatie.

Onderstaande tabel geeft u inzicht in de structurele kosten voor de MailReport dienstverlening.

| Aantal records per maand | Prijs in € per maand ex.btw | Opmerking |
|---|---|---|
| 0-50.000 | € 10,00 | 2 jaar retentie |
| 50.001-100.000 | € 15,00 | 2 jaar retentie |
| 100.001-500.000 | € 40,00 | 2 jaar retentie |
| 500.001-1.000.000 | € 75,00 | 2 jaar retentie |
| 1.000.001-5.000.000 | € 110,00 | 2 jaar retentie |
| 5.000.001-10.000.000 | € 170,00 | 2 jaar retentie |
| 10.000.001-50.000.000 | € 240,00 | 2 jaar retentie |
| 50.000.001-100.000.000 | € 300,00 | 2 jaar retentie |
| 100.000.001-500.000.000 | € 500,00 | 2 jaar retentie |
| 500.000.001-1.000.000.000 | € 700,00 | 2 jaar retentie |

Dit zijn prijzen per domein met bijbehorend volume aan records. Vrijwel alle aanbieders hanteren het volume per in kaart gebrachte emailbericht. Om u een indicatie te geven volgt hierbij een voorbeeld uit de praktijk over de kostenraming.

Voor een hele grote overheidsinstelling hebben we binnen een maand meer dan 5 miljoen emailberichten in kaart gebracht. Dit volume van 5 miljoen emailberichten is via verzamelde rapportages aangeleverd en verwerkt in iets meer dan 60.000 records.

**Links naar referentie materiaal**

- Pas toe of leg uit lijst van het Forum Standaardisatie
  https://lijsten.forumstandaardisatie.nl/open-standaard/dmarc
- Baseline Informatiebeveiliging Rijksdienst (BIR) & NEN-ISO/IEC 27001 en 27002
  http://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/inhoud/baseline-informatiebeveiliging-rijksdienst-bir--nen-iso-iec-27001-en-27002
- Factsheet Bescherm domeinnamen tegen phishing
  https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html
- RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  https://datatracker.ietf.org/doc/rfc7489/
- Anti-Phishing Best Practices for ISPs and Mailbox Providers
  https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

## VERSLEUTELING TUSSEN MAILSERVERS

Gebruikers melden zich vaak aan op een mailserver via een securechannel. Echter, veel communicatie tussen mailservers onderling is niet versleuteld. Hierdoor is het mogelijk dat uw emailbericht door derden wordt onderschept en kan worden gelezen. Laat ons helpen uw mailserver(s) op het juiste securityniveau te krijgen zodat u niet de zwakste schakel bent in de keten.

### Hoe doen we dit?

Wij zorgen ervoor dat uw mailserver een versleutelde verbinding kan opzetten en deze bij voorkeur ook gebruikt. De server waarmee uw server de verbinding wil gaan opzetten dient dit natuurlijk ook te ondersteunen. Deze techniek noemt men Secure SMTP over Transport Layer Security (TLS). Voor het versleutelen zijn certificaten op uw server(s) noodzakelijk. Als u DNSSEC heeft kunt u als extra toevoeging ook een zogenoemde fingerprint van het certificaat opnemen in een DNS record. De tegenpartij kan deze fingerprint opzoeken in DNS en verifiëren of het aangeboden certificaat hiermee overeenkomt. Deze techniek noemt men DANE.

### Wat zijn de voordelen?

Na invoering biedt Secure SMTP over TLS de onderstaande voordelen. Secure SMTP over TLS:

- verhoogt de privacy door versleuteling van het emailbericht tijdens transport;
- heeft geen impact op uw eindgebruiker;
- heeft geen invloed op verdere spamfilterafhandeling en content policy control;
- is een veilige en algemeen geaccepteerde manier van versleutelen;
- kan met SMTP over TLS de identiteit van de server worden geverifieerd wanneer de certificaten zijn gekocht van een officiële instantie (Certificate Authority). Wanneer men ook DANE met DNSSEC toepast kan via het certificaat ook de CA verifiëren worden geverifieerd;

Tevens:

- behoedt het u voor toekomstige aansprakelijkheid en de hieruit voortvloeiende claims (Wet Persoonsgegevens en Datalekken);
- bent u compliant met de pas toe of leg uit lijst (specifiek voor overheidsinstanties);
- bent u compliant met de BIR/BIG/BIWA (specifiek voor overheidsinstanties).

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

**Wat zijn de conclusies?**

- De emailberichten worden alleen tijdens transport versleuteld verstuurd tussen de servers onderling maar worden niet versleuteld opgeslagen op de servers zelf. Zo'n server kan ook dienen als tussenstop. De versleuteling is dus niet over het gehele traject tussen de verzender en ontvanger aanwezig;
- Verifieert niet de identiteit van de verzender. Het verifieert alleen de identiteit van de server waarmee de verzender zijn emailbericht verstuurt;
- Extra belasting van de server door het encrypten en decrypten van de emailberichten.

**Wat kost het?**

Om de ondersteuning om Secure SMTP over TLS, eventueel DNSSEC en DANE op orde te krijgen bieden wij u een vrijblijvende offerte aan op basis van fixed fee. De hoogte van de offerte is afhankelijk van de grootte en de complexiteit van uw organisatie. U kunt ook kiezen voor een aanbieding op basis van nacalculatie.

**Links naar referentiemateriaal**

- Forum Standaardisatie - Open standaarden – SMTP
  https://lijsten.forumstandaardisatie.nl/open-standaard/smtp
- Forum Standaardisatie - Open standaarden – TLS
  https://lijsten.forumstandaardisatie.nl/open-standaard/tls-0
- Forum Standaardisatie - Open standaarden – DANE
  https://lijsten.forumstandaardisatie.nl/open-standaard/dane
- ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)
  https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html
- Baseline Informatiebeveiliging Rijksdienst (BIR) & NEN-ISO/IEC 27001 en 27002
  http://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/inhoud/baseline-informatiebeveiliging-rijksdienst-bir--nen-iso-iec-27001-en-27002
- RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security
  https://datatracker.ietf.org/doc/rfc3207/
- RFC-7672 SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)
  https://datatracker.ietf.org/doc/rfc7672/?include_text=1

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

## VERSLEUTELING INDIVIDUELE EMAILBERICHTEN

Het basis emailprotocol (SMTP) stamt uit 1982 en wordt nog steeds gebruikt. In de tijd dat dit protocol is ontworpen hoefde men niet zoveel rekening te houden met beveiligingsaspecten zoals we die nu kennen. Op het SMTP protocol zijn later veel uitbreidingen verzonnen zoals ook secure SMTP over TLS (zie Versleuteling tussen mailservers) om het versturen van emailberichten veiliger te krijgen. Niet iedereen heeft deze uitbreidingen geïmplementeerd. De route die uw emailbericht volgt kan over meerdere mailservers lopen. De kans is aanwezig dat hier ook servers tussen zitten die geen versleuteling ondersteunen voor het transport. Ook de opslag op de mailservers zelf is niet versleuteld. Op de punten van de route waar u emailbericht niet versleuteld is zou men theoretisch uw emailbericht kunnen onderscheppen. Wanneer u vertrouwelijke emailbericht verstuurt is dit echter alleen te beveiligen door op individuele basis de emailberichten te versleutelen tussen de verzender en de ontvanger. Wij kunnen u hiermee op weg helpen.

### Hoe doen we dit?

Wij doen dit door de emailberichten op persoonsniveau te versleutelen. Hiervoor zijn twee varianten in omloop. De eerste is PGP (Pretty Good Privacy) en de tweede is S/MIME. Beiden werken volgens het zelfde principe van een publieke- en privésleutel. De PGP variant is met name populair binnen de opensource wereld. S/MIME wordt standaard ondersteunt binnen Microsoft Outlook. Op de werkplek van de verzender wordt het emailbericht versleuteld met behulp van de publieke sleutel van de ontvanger. De ontvanger kan het emailbericht op zijn werkplek decoderen met zijn eigen privésleutel. De verzender dient de publieke sleutel te bezitten van de ontvanger.

### Wat zijn de voordelen?

- Het emailbericht is tussen zender en ontvanger(s) volledig versleuteld;
- Verzender en ontvanger(s) zijn altijd bekend;
- Informatie kan niet tussen verzender en ontvanger(s) worden gelezen of gewijzigd;
- De eindgebruiker heeft controle wanneer hij iets versleuteld wil verzenden;
- Files/emailberichten worden versleuteld bewaard.

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

**Wat zijn de conclusies?**

- Sleutelmanagement is op eindgebruikers niveau dus voor een ICT afdeling bewerkelijk;
- Voor doorsnee eindgebruiker een behoorlijke leercurve om dit zelfstandig toe te passen;
- Van iedere ontvanger moet de verzender de publieke sleutel importeren;
- Indien men de privésleutel kwijtraakt is de versleutelde data niet meer toegankelijk;
- Emailverkeer tussen verschillende PGP implementaties is niet altijd onderling uitwisselbaar.

**Wat kost het?**

Waar (open)PGP vaak met zelf gegenereerde certificaten werkt, werkt S/MIME met officiële CA uitgegeven certificaten. Gelukkig kunt u via COMODO een gratis persoonlijk emailcertificaat krijgen.

S/MIME zit al in Outlook verwerkt en behoeft naast het importeren van het certificaat alleen maar aangezet te worden.

PGP vereist wat meer uitzoekwerk. Dit is ook afhankelijk welke implementatie uw ontvangers van PGP gebruiken. Voor PGP zijn open source en commerciële pakketten voorhanden.

Het implementeren van individuele emailversleuteling is bewerkelijk. De ondersteuning hiervoor gebeurt op basis van nacalculatie.

**Links naar referentiemateriaal**

RFC-5751 Secure/Multipurpose Internet Mail Extensions
https://tools.ietf.org/html/rfc5751

RFC-4880 OpenPGP Message Format
http://www.ietf.org/rfc/rfc4880.txt

Gaast 33
1274 AP Huizen
Nederland

+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

## BEGRIPPENLIJST

| | | |
|---|---|---|
| Authenticatie | = | Authenticatie is het proces waarbij iemand nagaat of een gebruiker, een andere computer of applicatie daadwerkelijk is wie hij beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken. |
| SPF | = | Afkorting van Sender Policy Frame |
| Sender Policy Framework | = | SPF is bedoeld om ongewenst verzenden van emailberichten namens jouw domeinnaam tegen te gaan. In een DNS record geef je aan de ontvanger aan welke servers (IP adressen) namens u emailberichten mogen verzenden. SPF is één van de authenticatiemechanieken van DMARC. |
| DKIM | = | Afkorting van DomainKeys Identified Mail |
| DomainKeys Identified Mail | = | DKIM biedt een basis voor authenticatie. DKIM voegt het veld "DKIM-Signature" toe aan de header van een emailbericht. Dit veld bevat een digitale handtekening van de inhoud van het emailbericht (op basis van zowel headers als de body van het emailbericht). De ontvangende SMTP-server controleert de DKIM-Signature met de publieke sleutel die via DNS opvraagbaar is. Als de controle slaagt betekent dat dat de emailbericht daadwerkelijk afkomstig is van het desbetreffende domein en niet aangepast is gedurende het transport. DKIM is één van de authenticatiemechanieken van DMARC. |
| DMARC | = | Afkorting van Domain-based Message Authentication, Reporting, and Conformance |
| Domain-based Message Authentication, Reporting, and Conformance | = | Het is een technische specificatie om phishing op domeinniveau tegen te gaan. De standaard is bedacht door een groep van grote technologiebedrijven waaronder Google, Microsoft, Yahoo, Facebook, Paypal en Bank of America. |
| DNS | = | Afkorting van Domain Name System |
| Domain Name System | = | DNS is het systeem en netwerkprotocol dat op het Internet gebruikt wordt om namen van computers naar numerieke adressen (IP-adressen) te vertalen en omgekeerd. |
| Phishing | = | Phishing is de verzamelnaam voor alle digitale activiteiten waarmee criminelen u proberen persoonlijke informatie te ontfutselen. Met deze informatie kan fraude met internetbankieren, pinpassen, creditcards of uw identiteit worden gepleegd. |
| Spambox | = | De map waar emailberichten worden bewaard die als ongewenst door het spamfilter zijn beoordeeld. |
| pas toe of leg uit lijst | = | Overheden en semi-overheden zijn verplicht de open standaarden, die op de lijst met 'pas toe of leg uit'-standaarden staan, bij aanschaf of (ver)bouw van ICT-systemen/-diensten te eisen ('pas toe'). Afwijken mag alleen met zwaarwegende redenen en verantwoording hierover |

Gaast 33
1274 AP Huizen
Nederland
+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

| | | |
|---|---|---|
| | | moet worden afgelegd in het jaarverslag ('leg uit'). |
| BIR | = | Afkorting van Baseline Informatiebeveiliging Rijksdienst |
| Baseline Informatiebeveiliging Rijksdienst | = | Door de toename van gegevensuitwisseling tussen ministeries is het binnen de rijksoverheid steeds belangrijker geworden om deze maatregelen te standaardiseren. De Baseline Informatiebeveiliging Rijksdienst (BIR) beschrijft deze algemeen te nemen maatregelen. Het BIR is gebaseerd op ISO 27001. |
| BIG | = | Afkorting van Baseline Informatiebeveiliging Nederlandse Gemeenten |
| Baseline Informatiebeveiliging Nederlandse Gemeenten | = | De BIG is afgeleid van de Baseline Informatiebeveiliging Rijksdienst (BIR) en voldoet aan de internationaal geaccepteerde beveiligingsstandaarden ISO 27001/27002. De BIG bestaat uit twee varianten, te weten de strategische BIG en de tactische BIG. Met de BIG kunnen gemeenten op een vergelijkbare manier efficiënt werken met informatiebeveiliging en hebben gemeenten een hulpmiddel om aan alle eisen ten aanzien van informatiebeveiliging te kunnen voldoen. |
| BIWA | = | Afkorting van Baseline Informatiebeveiliging Waterschappen |
| Baseline Informatiebeveiliging Waterschappen | = | De baseline bevat maatregelen die algemeen voorkomende informatiebeveiligingsrisico's bij de waterschappen afdekken. Hij bevat een aantal minimale beveiligingsniveaus waaraan een waterschap zou moeten willen voldoen. |
| SMTP | = | Afkorting van Simple Mail Transfer Protocol |
| Simple Mail Transfer Protocol | = | SMTP is de de facto-standaard voor het versturen van emailbericht over het internet. SMTP is een relatief simpel, tekst gebaseerd protocol: eerst wordt de afzender van het emailbericht gespecificeerd, daarna één of meerdere ontvangers en vervolgens de verzendgegevens en inhoud van het emailbericht. |
| TLS | = | Afkorting van Transport Layer Security |
| Transport Layer Security | = | TLS is een protocol de beveiliging van de communicatie verzorgt tussen client/server of server/server verbinding. Het garandeert de privacy, integriteit en beveiliging van de data die tussen servers worden verstuurd. |
| Fingerprint | = | Een fingerprint is a korte sequens van bytes die wordt gebruikt om de langere public key te kunnen identificeren. |
| DNSSEC | = | Is een samenvoeging van DNS en Secure. DNSSEC is een uitbreiding op DNS. DNSSEC verhelpt een aantal kwetsbaarheden in DNS waardoor de 'bewegwijzering' van het internet veiliger en vertrouwder wordt. |
| DANE | = | Afkorting van DNS-Based Authentication of Named Entities |
| DNS-Based Authentication of Named Entities | | DANE is uitbreiding van DNSSEC. Daarmee kunnen sleutels en certificaten voor beveiligde verbindingen naar websites of mailservers in het DNS-systeem worden opgenomen. |
| CA | = | Afkorting van Certificate Authority |
| Certificate Authority | = | Officiële instantie die gemachtigd is om certificaten uit te geven en te onderschrijven. Bij de CA kun je controleren of het |

Gaast 33
1274 AP Huizen
Nederland
+31 6 136 17 631
contact@substructure.nl
www.substructure.nl

certificaat geldig is en door hun is verstrekt.

| | | |
|---|---|---|
| Certificaten | = | Het certificaat zorgt voor decryptie van de verbinding en voor het valideren van de identiteit van een website. Het certificaat bevat onder andere informatie over:<br>• De certificaathouder<br>• Servernaam en domein<br>• De naam van de Certificate Authority (CA) die het certificaat heeft uitgegeven<br>• Het root certificaat<br>• Het land waarin het certificaat is uitgegeven<br>• De geldigheidsduur<br>• Een certificaat bestaat altijd uit een Publieke sleutel en een Privésleutel. |
| Decryptie | = | Het leesbaar maken van versleutelde gegevens |
| Encryptie | = | Het versleutelen van gegevens |
| Versleutelen | = | Binnen de cryptografie staat versleutelen voor het coderen (encryptie) van gegevens op basis van een bepaald algoritme. Deze versleutelde gegevens kunnen nadien weer gedecrypteerd (ontcijferd of gedecodeerd) worden zodat men de originele informatie weer terugkrijgt. Dit proces wordt decryptie genoemd.<br><br>Eén van de bedoelingen van cryptografie is dat gegevens veilig uitgewisseld kunnen worden tussen twee personen / servers over een onveilig communicatiekanaal, dat wil zeggen een communicatiekanaal waar ook derden toegang toe kunnen hebben, zoals het internet. De versleuteling zorgt er dan voor dat deze derden de gegevens niet kunnen lezen. Dit gebeurt meestal door het gebruik van sleutels. Wat precies een sleutel vormt verschilt per algoritme, maar meestal is een sleutel een bepaald heel groot getal van enkele tientallen decimalen. Het doel van het cryptografische algoritme is dan om er voor te zorgen dat alleen de personen met de juiste sleutel de versleutelde gegevens weer kunnen ontcijferen. |
| Publieke sleutel | = | De verzender gebruikt de publieke sleutel die de ontvanger hem heeft verstrekt om emailberichten aan ontvanger te coderen. |
| Privésleutel | = | De ontvanger kan met deze sleutel emailberichten die met zijn publieke sleutel zijn versleuteld decrypten. |
| S/MIME | = | Standaard voor het versleutelen van individuele emailberichten deze standaard word vooral door Microsoft ondersteund. |
| PGP | = | Afkorting van Pretty Good Privacy |
| Pretty Good Privacy | = | Standaard voor het versleutelen van individuele emailberichten. |