Opzetten beveiligde e-mail verbinding met DNB

DNB streeft ernaar om bedrijfsgevoelige informatie altijd via beveiligde e-mail uit te wisselen met de instellingen die onder haar toezicht staan. Reden is dat onbeveiligde e-mail onvoldoende garantie biedt dat de informatie-uitwisseling rechtstreeks verloopt zonder tussenkomst van onbevoegden.

DNB ondersteunt meerdere vormen van beveiligde e-mail. Welke oplossing voor u het meest geschikt is, zal afhangen van uw specifieke voorkeuren en de financiële en organisatorische consequenties voor uw instelling.

De volgende gateway-to-gateway protocollen worden door DNB ondersteund:

1. S/MIME (Deze oplossing heeft de voorkeur van DNB).
S/MIME (Secure/Multipurpose Internet Mail Extensions) is een standaard voor het beveiligd verzenden van e-mail dat in een MIME-structuur is gevat. S/MIME gebruikt asymmetrische cryptografie met een publieke sleutel om het bericht te versleutelen en digitaal te ondertekenen. S/MIME is een veilige manier van e-mailverzending.

2. PGP
PGP (dit staat voor Pretty Good Privacy) is gebaseerd op een schema van asymmetrische cryptografie. Dit houdt in dat er twee verschillende sleutels zijn, één voor vercijferen en één voor ontcijferen van de informatie. PGP is een veilige manier van e-mailverzending.

3. Forced TLS i.c.m. verifiëren en valideren van het certificaat
Bij TLS (Transport Layer Security) wordt de e-mail zelf niet versleuteld maar de netwerkverbinding tussen verzender en ontvanger wordt versleuteld. Om er zeker van te zijn dat de e-mail bij de juiste partij wordt afgeleverd, wordt er gebruik gemaakt van verifiëren en valideren van het certificaat.