Voorwoord

Vandaag de dag maken bedrijven vaak gebruik van e-mail, een communicatiemiddel dat voor de uitwisseling van informatie gebruikt wordt.

Ook de ondernemingsgroep ALDI Nord houdt via e-mail contact met een groot aantal communicatiepartners.
Aangezien de informatie die via e-mail uitgewisseld wordt, meestal vertrouwelijk is, moet deze beschermd worden tegen toegang door onbevoegden vooraleer ze behandeld kan worden. Zonder een afzonderlijke beveiliging is de dataoverdracht via internet tussen afzender en ontvanger volledig onbeveiligd en vergelijkbaar met het versturen van een postkaart.
Om de e-mailcommunicatie effectief te beschermen, zijn extra veiligheidsmaatregelen nodig.
Om vertrouwelijke informatie in e-mails te beveiligen, past de ondernemingsgroep ALDI Nord veilige standaardprocedures voor de uitwisseling van gecodeerde e-mails toe.

De ondernemingsgroep ALDI Nord wil u via dit document alle informatie verstrekken die vereist is om een veilige communicatie tussen u en ALDI Nord tot stand te kunnen brengen.

Op de volgende pagina's worden de relevante begrippen beschreven die betrekking hebben op de e-mailcodering en de fundamentele stappen voor de configuratie en het opzetten van een veilig communicatiesysteem.

Vervolgens worden twee mogelijkheden voorgesteld aan de hand waarvan u met ALDI Nord een gecodeerde communicatie kan initialiseren. Op het einde van dit document vindt u hieromtrent een korte handleiding.

Gelieve u bij vragen over de e-mailcodering in combinatie met de in uw bedrijf gebruikte e-mailoplossing te wenden tot de desbetreffende technische contactpersoon in uw bedrijf.

Codering

Om de vertrouwelijkheid van een e-mailcommunicatie te garanderen, moeten e-mails gecodeerd worden.
De vereiste informatie om e-mails te coderen en te decoderen, is opgenomen in een zogenaamd certificaat dat de publieke sleutel (voor alle communicatiepartners) voor de codering en de private sleutel (enkel voor de eigenaar) voor de codering bevat. Voordat een veilige uitwisseling van informatie in de vorm van een gecodeerde e-mail kan plaatsvinden, moeten beide communicatiepartners over de publieke sleutel van de ander beschikken.

Publieke en private sleutels

Een certificaat bestaat uit twee delen: een publieke en een private sleutel.
De private sleutel wordt gebruikt voor het ondertekenen en decoderen van e-mails en mag niet openbaar gemaakt worden.
De publieke sleutel moet ter beschikking gesteld worden van de communicatiepartner zodat hij/zij de handtekening van een e-mail kan controleren en gecodeerde e-mails naar de eigenaar van de publieke sleutel kan versturen.

Voordat de eerste e-mail gecodeerd wordt, moet de zender de publieke sleutel als deel van het certificaat van de ontvanger van de e-mail ontvangen hebben.
Deze uitwisseling vindt normaal plaats in de vorm van een ondertekende e-mail waarin de ontvanger de publieke sleutel kan terugvinden. Pas dan kan de afzender de e-mail met de publieke sleutel van de ontvanger coderen.
Nadat hij/zij de gecodeerde e-mail ontvangen heeft, kan de ontvanger deze met zijn private sleutel decoderen. Deze processen worden door de meeste e-mailprogramma's automatisch uitgevoerd.

Handtekeningen

Om de echtheid van een e-mailadres automatisch te kunnen controleren, is een digitale handtekening vereist. Via deze handtekening kan de afzender van de e-mail duidelijk geïdentificeerd worden.
Bovendien wordt dankzij deze handtekening gegarandeerd dat de e-mail onbeschadigd is. Als de inhoud van de e-mail achteraf gewijzigd wordt, is de digitale handtekening verstoord, net als bij een gebroken zegel van een brief.
Bij de ondertekening van een e-mail wordt daarom altijd de publieke sleutel van het certificaat bij de e-mail bijgevoegd zodat de ontvanger de e-mail onmiddellijk kan controleren op echtheid en ongeschondenheid.
Door een e-mail te ondertekenen, kan de informatie in de e-mail niet gewijzigd worden zonder dat de ontvanger dit merkt. De e-mail blijft wel leesbaar. Om het vertrouwelijke karakter van de informatie-uitwisseling te garanderen, moet de e-mail extra gecodeerd worden. De veiligste manier om e-mails te versturen is via een combinatie van handtekening en codering.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is een wereldwijd gebruikte standaardprocedure voor de beveiligde uitwisseling van informatie via e-mail met certificaten. De vereiste onderdelen voor S/MIME zijn reeds in de meeste moderne e-mailprogramma's geïntegreerd zodat een eenvoudig en transparant gebruik ervan gegarandeerd is. Dit betekent dat e-mails door de activering van de respectievelijke opties in het e-mailprogramma voor het

versturen van de e-mail automatisch gecodeerd en bij ontvangst automatisch gedecodeerd worden.
De ondernemingsgroep ALDI Nord aanvaardt enkel de S/MIME-procedure voor de e-mailcodering.

Certificaataanbieders/trustcenters

Een certificaataanbieder (ook trustcenter genoemd) is een organisatie die digitale gebruikerscertificaten aanbiedt en verantwoordelijk is voor hun beschikbaarstelling, toewijzing en de beveiliging van hun integriteit.
Indien u over een e-mailsysteem met S/MIME beschikt, maar nog geen eigen certificaat heeft, kan u dit bij een certificaataanbieder aanvragen. Als bijlage vindt u een overzicht van aanbieders die de ondernemingsgroep ALDI Nord vertrouwt.

Stamcertificaat

Naast het certificaat van de desbetreffende gebruiker is bij de e-mailcommunicatie met de ondernemingsgroep ALDI Nord ook een zogenaamd stamcertificaat vereist. Via dit certificaat kan de betrouwbaarheid van de certificaten van de ondernemingsgroep ALDI Nord gecontroleerd worden.
Dit betekent dat het door u gebruikte systeem kan controleren of het certificaat daadwerkelijk afkomstig is van de ondernemingsgroep ALDI Nord en of het nog geldig is.

Uitwisseling van certificaten

De communicatiepartners moeten de certificaten slechts één keer voor de eerste codering uitwisselen. Daarna is uitwisseling pas opnieuw nodig als een van de uitgewisselde certificaten niet meer geldig is.

Certificaat aan de ondernemingsgroep ALDI Nord bezorgen:
Als u uw persoonlijk certificaat ontvangen heeft van een certificaataanbieder/trustcenter uit de lijst in de bijlage en u uw publieke sleutel op de keyserver van de certificaataanbieder/het trustcenter (vgl. handleiding, hoofdstuk 2.1) opgeslagen heeft, wordt uw publieke sleutel door de keyserver van de certificaataanbieder/het trustcenter automatisch opgevraagd.
Als u uw publieke sleutel niet op de keyserver van uw certificaataanbieder/trustcenter opgeslagen heeft, kan u deze via het ALDI-certificaatportaal (www.aldi-nord.de/certportal) uploaden.

Als uw gebruikerscertificaat gewijzigd werd, bv. omdat u van certificaataanbieder veranderd bent, moet u deze werkwijze herhalen.

Certificaten van de ondernemingsgroep ALDI Nord ontvangen:
Het desbetreffende gebruikerscertificaat ontvangt u automatisch per versleutelde e-mail van uw contactpersoon in de ondernemingsgroep ALDI Nord. Bovendien kan u via het ALDI-certificaatportaal (www.aldi-nord.de/certportal) certificaten van uw contactpersonen downloaden met vermelding van het exacte e-mailadres.
Het stamcertificaat, dat uw contactpersoon bij ALDI Nord u eveneens per versleutelde e-mail doorstuurt, moet eenmalig op uw toestel (bv. pc) geïmporteerd worden voor de controle van de gebruikerscertificaten van de ondernemingsgroep ALDI Nord.
Het gebruikerscertificaat moet toegewezen worden aan de respectievelijke contactpersoon in het gebruikte e-mailprogramma (vgl. handleiding, hoofdstuk. 2.5).

Het stamcertificaat van de ondernemingsgroep ALDI Nord kan via het ALDI-certificaatportaal (www.aldi-nord.de/certportal) alsook via het adres www.aldi-nord.de/cert/ gedownload worden of u ontvangt het automatisch per gecodeerde e-mail (als bijlage) van uw contactpersoon bij ALDI Nord (vgl. handleiding, hoofdstuk 4).

Webmessenger

Via een portaal of webmessenger krijgt een communicatiepartner via een beveiligde internetverbinding toegang tot een e-mailclient. Via de door ALDI Nord ter beschikking gestelde e-mailclient heeft de communicatiepartner de mogelijkheid om e-mails naar medewerkers van ALDI te versturen of e-mails van medewerkers van ALDI te ontvangen.

Hierna worden de verschillende stappen van de beveiligde communicatie met ALDI Nord nogmaals weergegeven. Voor een optimaal gebruik van de beveiligde e-mailcommunicatie bevelen wij mogelijkheid 1 aan.

1e mogelijkheid:

U heeft tot nu toe nog geen beveiligd contact gehad met ALDI Nord (ook geen webmessenger-toegang) en wilt in de toekomst gecodeerde e-mails met ALDI Nord uitwisselen (uitwisseling van sleutels via publicatie van de publieke sleutel op de keyserver van de certificaataanbieder/het trustcenter).

1	**Vraag** een persoonlijk S/MIME-e-mailcertificaat **aan** bij een trustcenter uit de lijst in de bijlage (publiceer uw publieke sleutel op de keyserver van het trustcenter) (vgl. handleiding hoofdstuk 2.1 en 2.2)
2	**Toewijzing** van het certificaat aan de persoonlijke e-mailaccount in de opties van de door u gebruikte e-mailsoftware (vgl. handleiding hoofdstuk 2.4)
3	**ALDI Nord** controleert de keyservers van de in de lijst vermelde trustcenters en gebruikt uw publieke sleutel (u hoeft hiervoor niets te doen)
4	**Ontvangst** van een gecodeerde e-mail van uw contactpersoon bij ALDI Nord. De e-mail bevat het certificaat van de ALDI-contactpersoon en het stamcertificaat van ALDI Nord.
5	**Aanmaken** van een contact voor de contactpersoon bij ALDI Nord in het e-mailprogramma en toewijzen van het desbetreffende certificaat aan het gecreëerde contact (vgl. handleiding hoofdstuk 2.5)
6	**Selectie** van de coderingsoptie S/MIME bij het opstellen van een e-mail voor de ALDI-contactpersoon (vgl. handleiding hoofdstuk 2.4)

2e mogelijkheid:

U heeft van een ALDI-contactpersoon toegang tot webmessenger verkregen en kan hiermee gecodeerde e-mails naar ALDI-contactpersonen versturen.

Ondersteunende certificaataanbieders/trustcenters:

Swiss Sign	https://www.swisssign.com
Product:	Personal ID Silver
Opmerking:	De certificaten zijn ook buiten Zwitserland geldig.

Vertrouwde stamcertificaten zijn o.a.:

SwissSign Gold CA
SwissSign Gold CA G2
SwissSign Gold Root CA
SwissSign Gold Personal CA G3
SwissSign Silver CA G2
SwissSign Silver Root CA
SwissSign Silver Personal CA G3

Stamcertificaten van ALDI Nord en controlesommen

1. ALDI Nord
   S/MIME stamcertificaat
   Geldig vanaf 04.12.2015

   SHA1: `a06a c71d b800 e8d9 56c3 c3e5 9ed0 bc3f 0ce0 b6d3`
   MD5: `bfd1 22f4 f721 197c 0860 38fc eef2 0752`

2. ALDI Nord
   S/MIME stamcertificaat
   Geldig tot 06.01.2016

   SHA1: `e072 577b 2bd8 f68a ee6b eba2 17ca e9b6 b7a6 ba43`
   MD5: `542b b140 189c 0d0a d146 0007 e677 a6ed`