Forord

De fleste virksomheder i dag benytter e-mail som kommunikationsmiddel, når der skal udveksles informationer.

Virksomhedsgruppen ALDI Nord (herefter benævnt ALDI) er også i e-mail-kontakt med flertallet af deres kommunikationspartnere.
Informationerne, som bliver udvekslet pr. e-mail, er ofte fortrolige, hvilket betyder, at de skal beskyttes mod manipulation og fremmed adgang. Uden særlig sikring er dataoverførslen mellem afsender og modtager via internettet fuldstændig ubeskyttet og at sammenligne med afsendelsen af et postkort.
For at sikre en effektiv beskyttelse af e-mail-kommunikationen, er det derfor nødvendigt med yderligere sikkerhedsforanstaltninger.
For at beskytte fortrolige informationer i e-mails benytter ALDI en sikker standardiseret metode til udveksling af kryptede e-mails.

Med dette dokument vil ALDI gerne stille de relevante informationer til rådighed, som er nødvendige for at kunne opbygge en sikker kommunikationsvej mellem dig og ALDI.

I det følgende vil de relevante begreber i forbindelse med e-mail-kryptering og de grundlæggende skridt til konfiguration og indretning af et sikkert kommunikationssystem blive gennemgået.

Afslutningsvis vil 2 varianter blive introduceret, således at du kan initialisere krypteret kommunikation med ALDI. I slutningen af dette dokument finder du en kort vejledning til brug for dette.

Såfremt du har spørgsmål til e-mail-kryptering i det e-mail-program, der er i din virksomhed, bedes du henvende dig til din egen IT-afdeling.

Kryptering

For at bevare fortroligheden i e-mail-kommunikationen skal e-mailene krypteres.
De nødvendige informationer, som skal benyttes til kryptering og dekryptering af e-mails, er indeholdt i et såkaldt certifikat, som indeholder den offentlige nøgle (til alle kommunikationspartnere) til kryptering og den private nøgle (kun til brugeren) til dekryptering. Før en sikker udveksling af informationer i form af krypterede e-mails kan finde sted, må begge parter være i besiddelse af et digitalt certifikat.

Offentlig og privat nøgle

Et certifikat består af 2 dele: en offentlig og en privat nøgle.
Den privat nøgle bliver brug til signering og dekryptering af e-mails og må ikke offentliggøres.
Den offentlige nøgle stilles til rådighed for eksterne partnere, hvorved de kan kontrollere e-mailens digitale signatur og sende krypterede e-mails til indehaveren af den offentlige nøgle.

Før den første kryptering af e-mails må afsenderen modtage den offentlige nøgle som er en del af modtagerens certifikat. Denne udveksling sker som regel gennem fremsendelse af en digitalt signeret e-mail, som modtageren af den offentlige nøgle kan se. Først derefter kan afsenderen kryptere e-mailen med modtagerens offentlige nøgle.
Efter modtagelse af den krypterede e-mail kan modtageren med sin private nøgle dekrypterere e-mailen. Disse processer vil automatisk blive gennemført i de fleste e-mail-programmer.

Signatur

For at en e-mailadresses ægthed automatisk kan blive kontrolleret, benyttes der en digital signatur. Ved hjælp af denne kan afsendelsen af en e-mail tydeligt identificeres.
Derudover garanterer den digitale signatur for, at e-mailens indhold ikke er blevet ændret, fordi den digitale signatur vil blive ødelagt, såfremt der er foretaget en efterfølgende ændring i indholdet/dataene – det kan sammenlignes med et brudt segl på et brev.
Ved digital signering af en e-mail bliver certifikatets offentlige nøgle derfor altid vedhæftet e-mailen, således at modtageren kan kontrollere e-mailens ægthed, og at den ikke er blevet ændret.
Gennem e-mailens digitale signering kan informationerne, der er i e-mailen, ikke ændres uden at modtageren bemærker dette. Meddelelsens indhold er imidlertid stadigvæk almindelig læsbar. For at bevare fortroligheden ved informationsudveksling må e-mailsene derfor krypteres. Den sikreste metode til udveksling af e-mails er kombinationen af digital signatur og kryptering.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) er en world-wide uafhængig standardprocedure for sikker udveksling af informationer pr. e-mail med certifikat. De nødvendige komponenter for S/MIME er allerede integreret i de fleste moderne e-mail-programmer, således at der er sikret en enkel og transparent håndtering. Det betyder at e-mails, gennem aktivering af valgmuligheden i e-mail-programmet, før afsendelsen automatisk bliver krypteret og ved modtagelsen automatisk dekrypteret.

ALDI accepterer udelukkende S/MIME-funktionen til e-mail-kryptering.

Certifikatudbyder/trustcenter

En certifikatudbyder (også kaldet et trustcenter) er en organisation, som udsteder digitale brugercertifikater, og som er ansvarlig for leveringen, fordelingen og integritetssikkerheden.
Såfremt du råder over et e-mail-system med S/MIME-funktion, men endnu ikke har dit eget certifikat, kan du ansøge om et sådant hos en certifikatudbyder. En oversigt over udbydere, som ALDI har tillid til, findes i det tilhørende bilag.

Stamcertifikat

For at kunne e-mail-kommunikere med ALDI skal der foruden certifikatet også benyttes et såkaldt stamcertifikat. Med stamcertifikatet er det muligt at kontrollere tillidsstatussen på ALDIs certifikater.
Det betyder, at det af system, som du anvender, kan kontrollere, om certifikatet virkelig stammer fra ALDI og stadig er gyldigt.

Certifikatudveksling

Certifikatudvekslingen mellem kommunikationspartnerne skal kun gennemføres én gang før den første kryptering og er derefter først nødvendig igen, når gyldigheden på et af de udvekslede certifikater udløber.

Transmission af certifikat til ALDI:
Når du har modtaget dit personlige certifikat fra en af certifikatudbydere på oversigten fra bilaget og deponeret din offentlige nøgle på certifikatudbyderens nøgleserver (jfr. vejledningens kapitel 2.1), vil din offentlige nøgle fra certifikatudbyderens/trustcentrets nøgleserver automatisk blive modtaget.
Såfremt du ikke har offentliggjort din offentlige nøgle på certifikatudbyderens nøgleserver, kan du downloade den fra ALDIs certifikatsportal (www.aldi-nord.de/certportal).

Såfremt du har ændret dit brugercertifikat, fx på grund af udskiftning af dit certifikatudbyder, må du gentage denne proces.

Modtagelse af ALDIs certifikat:
Du vil automatisk modtage det respektive brugercertifikat med den krypterede e-mail fra din kommunikationspartner hos ALDI. Certifikater fra dine kontaktpersoner hos ALDI kan ligeledes downloades fra ALDIs certifikatsportal (www.aldi-nord.de/certportal) efter angivelse af den eksakte e-mail-adresse.
Stamcertifikatet, som du ligeledes automatisk vil få med e-mailen fra din kommunikationspartner hos ALDI, skal importeres en gang for alle til din slutenhed (fx. PC), således at der kan gennemføres kontrol af ALDIs brugercertifikat.
Brugercertifikatet skal tildeles den respektive kontakt i det benyttede e-mail-program (jfr. vejledningens kapitel 2.5).
ALDIs stamcertifikat kan enten downloades fra ALDIs certifikatsportal (www.adi-nord.de/certportal/), via adressen www.aldi-nord.de/cert/ eller du modtager det automatisk med den krypterede e-mail (som

bilag) fra din kommunikationspartner hos ALDI (jfr. vejledningens kapitel 4).

Webmessenger

Via en sikker internetforbindelse modtager en kommunikationspartner ved hjælp af en portal eller webmessenger adgang til en e-mail-klient. Ved hjælp af den e-mail-klient, som ALDI stiller til rådighed, har kommunikationspartneren mulighed for at sende og modtage sikre e-mails til og fra ALDI-medarbejdere.

I det følgende vil afviklingen af krypteret kommunikation med ALDI igen blive gennemgået. For optimal brug af sikker e-mail-kommunikation anbefales variant 1.

1. variant:

Du har ikke tidligere haft sikker e-mail-kontakt med ALDI (heller ikke via webmessenger-adgang) og vil gerne fremover benytte krypteret e-mail-kommunikation med ALDI (nøgleudveksling gennem publikation af den offentlige nøgle på certifikatudbyderens nøgleserver).

1	**Ansøg** om et personligt S/MIME-e-mail-certifikat hos en af certifikatudbyderne på oversigten i bilaget (publicer din offentlige nøgle på certifikatudbyderens nøgleserver (jfr. vejledningens kapitel 2.1 og 2.2).
2	**Overdrag** certifikatet til den personlige e-mail-konto i optionerne i det af dig valgte e-mail-software (jfr. vejledningens kapitel 2.4).
3	**ALDI** retter en forespørger til nøgleserveren hos den valgte certifikatudbyder og gemmer din offentlige nøgle (du behøver ikke at foretage dig noget).
4	**Modtag** en sikker e-mail fra din kommunikationspartner hos ALDI. E-mailen indeholder kommunikationspartnerens certifikat og ALDIs stamcertifikat.
5	**Opret** en kontakt på ALDIs kommunikationspartner i e-mail-programmet og tildel det tilhørende certifikat til den oprettede kontakt (jfr. vejledningens kapitel 2.5).
6	**Udvælg** krypteringsoption S/MIME ved at skrive en e-mail til din ALDI kommunikationspartner (jfr. vejledningens kapitel 2.4).

2. variant:

Du har modtaget adgang til webmessenger fra ALDIs kommunikationspartner og kan herigennem sende sikre e-mails til ALDIs kommunikationspartner.

Liste over understøttede certifikatudbydere/trustcentre:

Swiss Sign	https://www.swisssign.com/
Produkt:	Personal ID Silver
Hinvisning:	Certifikaterne er også gyldige udenfor Schweiz.
Godkendte Stamcertifikater:	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

ALDI Nord rodcertifikater og checksum

1. ALDI Nord
S/MIME rodcertifikat
Gyldig fra 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 rodcertifikat
Gyldig til 06.01.2016

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