## Vorwort

E-Mail ist heute für Unternehmen ein häufig eingesetztes Kommunikationsmittel, das zum Austausch von Informationen verwendet wird.

Auch die Unternehmensgruppe ALDI Nord steht mit einer Vielzahl von Kommunikationspartnern per E-Mail in Kontakt.
Die Informationen, die über E-Mail ausgetauscht werden, sind dabei meist auch vertraulich, sodass sie besonders vor Manipulation und fremdem Zugriff geschützt werden müssen. Ohne eine gesonderte Absicherung ist die Datenübermittlung im Internet zwischen Absender und Empfänger völlig ungeschützt und vergleichbar mit dem Versand einer Postkarte.
Für einen wirkungsvollen Schutz der E-Mail-Kommunikation sind deshalb zusätzliche Sicherheitsmaßnahmen zwingend erforderlich.
Um vertrauliche Informationen in E-Mails zu schützen, verwendet die Unternehmensgruppe ALDI Nord sichere Standardverfahren zum Austausch von verschlüsselten E-Mails.

Die Unternehmensgruppe ALDI Nord möchte Ihnen mit diesem Dokument alle Informationen bereitstellen, die notwendig sind, um einen sicheren Kommunikationsweg zwischen Ihnen und ALDI Nord aufbauen zu können.

Im Folgenden werden die relevanten Begriffe im Zusammenhang mit E-Mail-Verschlüsselung und die grundlegenden Schritte zur Konfiguration und Einrichtung eines sicheren Kommunikationssystems erläutert.

Anschließend werden zwei Varianten vorgestellt, wie Sie mit ALDI Nord eine verschlüsselte Kommunikation initialisieren können. Am Ende dieses Dokuments finden Sie hierzu eine kurze Anleitung.

Bei Fragen bezüglich E-Mail-Verschlüsselung in Verbindung mit der in Ihrem Unternehmen eingesetzten E-Mail-Lösung wenden Sie sich bitte an die entsprechenden technischen Ansprechpartner in Ihrem Unternehmen.

## Verschlüsselung

Um die Vertraulichkeit einer E-Mail-Kommunikation zu wahren, müssen E-Mails verschlüsselt werden.
Die notwendigen Informationen, die zum Ver- und Entschlüsseln von E-Mails benötigt werden, sind in einem sogenannten Zertifikat enthalten, welche den öffentlichen Schlüssel (für alle Kommunikationspartner) für die Verschlüsselung und den privaten Schlüssel (nur für den Besitzer) für die Entschlüsselung beinhaltet. Somit müssen bevor ein gesicherter Austausch von Informationen in Form von verschlüsselten E-Mails stattfinden kann, beide Kommunikationspartner über den öffentlichen Schlüssel des Gegenübers verfügen.

## Öffentliche und private Schlüssel

Ein Zertifikat besteht aus zwei Teilen: einem öffentlichen und einem privaten Schlüssel.
Der private Schlüssel wird für die Signierung und Entschlüsselung von E-Mails verwendet und darf nie veröffentlicht werden.
Der öffentliche Schlüssel muss dem Kommunikationspartner zur Verfügung gestellt werden, damit er die Signatur einer E-Mail überprüfen und verschlüsselte E-Mails an den Besitzer des öffentlichen Schlüssels versenden kann.

Vor der ersten Verschlüsselung von E-Mails muss der Absender den öffentlichen Schlüssel als Teil des Zertifikats des Empfängers der E-Mail erhalten haben. Dieser Austausch erfolgt in der Regel durch den Versand einer signierten E-Mail, der der Empfänger den öffentlichen Schlüssel entnehmen kann. Erst dann kann der Absender die E-Mail mit dem öffentlichen Schlüssel des Empfängers verschlüsseln.
Nach dem Erhalt der verschlüsselten E-Mail kann der Empfänger diese mit seinem privaten Schlüssel entschlüsseln. Diese Vorgänge werden von den meisten E-Mail-Programmen automatisch durchgeführt.

## Signaturen

Damit die Echtheit einer E-Mail-Adresse automatisch überprüft werden kann, wird eine digitale Signatur benötigt. Durch sie kann der Absender einer E-Mail eindeutig identifiziert werden.
Außerdem wird mit ihr die Unversehrtheit der E-Mail garantiert, da bei einer nachträglichen Änderung der Daten die digitale Signatur – ähnlich einem gebrochenen Siegel eines Briefes – zerstört wird.
Beim Signieren einer E-Mail wird deshalb immer der öffentliche Schlüssel des Zertifikats an die E-Mail angehängt, damit der Empfänger die Echtheit und Unversehrtheit der E-Mail prüfen kann.
Durch die Signierung einer E-Mail können die darin enthaltenen Informationen nicht geändert werden, ohne dass es der Empfänger bemerkt. Sie sind aber weiterhin offen lesbar. Um die Vertraulichkeit beim Informationsaustausch zu gewährleisten, muss die E-Mail zusätzlich verschlüsselt werden. Das sicherste Verfahren zum Austausch von E-Mails ist die Kombination von Signatur und Verschlüsselung.

## S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) ist ein weltweit eingesetztes Standardverfahren für den gesicherten Austausch von Informationen per E-Mail mit Zertifikaten. Die notwendigen Komponenten für S/MIME sind in den meisten modernen E-Mail-Programmen bereits integriert, sodass eine einfache und transparente Handhabung gewährleistet ist. Das bedeutet, dass E-Mails durch die Aktivierung der entsprechenden Option im E-Mail-Programm vor dem Versand automatisch verschlüsselt und beim Empfang automatisch entschlüsselt werden.

Die Unternehmensgruppe ALDI Nord akzeptiert ausschließlich das S/MIME-Verfahren zur E-Mail-Verschlüsselung.

## Zertifikatsdiensteanbieter/Trustcenter

Ein Zertifikatsdiensteanbieter (auch Trustcenter genannt) ist eine Organisation, die digitale Benutzerzertifikate herausgibt und für deren Bereitstellung, Zuweisung und Integritätssicherung verantwortlich ist.
Sofern Sie über ein S/MIME-fähiges E-Mail-System verfügen, aber noch kein eigenes Zertifikat besitzen, können Sie dieses bei einem Zertifikatsdiensteanbieter beantragen. Eine Übersicht von Anbietern, der die Unternehmensgruppe ALDI Nord vertraut, finden Sie im Anhang.

## Stammzertifikat

Zusätzlich zu dem Zertifikat des jeweiligen Benutzers wird bei der E-Mail-Kommunikation mit der Unternehmensgruppe ALDI Nord auch ein sogenanntes Stammzertifikat benötigt. Mit diesem kann der Vertrauensstatus der Zertifikate der Unternehmensgruppe ALDI Nord überprüft werden.
Das bedeutet, dass das von Ihnen eingesetzte System überprüfen kann, ob das Zertifikat wirklich von der Unternehmensgruppe ALDI Nord stammt und ob es noch gültig ist.

## Zertifikatsaustausch

Der Zertifikatsaustausch zwischen den Kommunikationspartnern muss nur einmal vor dem ersten Verschlüsseln durchgeführt werden und ist danach erst wieder notwendig, wenn eines der ausgetauschten Zertifikate seine Gültigkeit verliert.

Zertifikat an die Unternehmensgruppe ALDI Nord übermitteln:
Wenn Sie Ihr persönliches Zertifikat von einem der Zertifikatsdiensteanbieter/Trustcenter aus der Liste im Anhang erhalten und Ihren öffentlichen Schlüssel auf dem Keyserver des Zertifikatsdiensteanbieters/Trustcenters (vgl. Anleitung Kap. 2.1) hinterlegt haben, wird Ihr öffentlicher Schlüssel von dem Keyserver des Zertifikatsdiensteanbieters/Trustcenters automatisch abgefragt.
Wenn Sie Ihren öffentlichen Schlüssel nicht auf dem Keyserver des Zertifikatsdiensteanbieters/Trustcenters veröffentlicht haben, können Sie diesen über das ALDI Zertifikatsportal (www.aldi-nord.de/certportal) bereitzustellen.

Wenn sich Ihr Benutzerzertifikat geändert hat, z. B. aufgrund des Wechsels Ihres Zertifikatsanbieters, müssen Sie diesen Vorgang wiederholen.

Zertifikate von der Unternehmensgruppe ALDI Nord erhalten:
Das jeweilige Benutzerzertifikat erhalten Sie automatisch mit jeder verschlüsselt empfangener E-Mail von Ihrem Kommunikationspartner in der Unternehmensgruppe ALDI Nord. Zudem können Sie Zertifikate Ihrer Kontaktpersonen bei ALDI über das ALDI Zertifikatsportal (www.aldi-nord.de/certportal) unter Angabe der exakten E-Mail-Adresse herunterladen.
Das Stammzertifikat, welches Ihnen ebenfalls automatisch mit einer verschlüsselten E-Mail von Ihrem Kommunikationspartner bei ALDI Nord zugeht, muss für die Überprüfung der Benutzerzertifikate der Unternehmensgruppe ALDI Nord auf Ihrem Endgerät (z. B. PC) einmalig importiert werden.
Das Benutzerzertifikat ist dem entsprechenden Kontakt in dem eingesetzten E-Mail-Programm zuzuordnen (vgl. Anleitung Kap. 2.5).
Das Stammzertifikat der Unternehmensgruppe ALDI Nord kann über das ALDI Zertifikatsportal (www.aldi-nord.de/certportal) sowie unter der Adresse www.aldi-nord.de/cert/ heruntergeladen werden oder Sie erhalten es automatisch mit jeder verschlüsselten E-Mail (als Anhang) von Ihrem Kommunikationspartner bei ALDI Nord (vgl. Anleitung Kap. 4).

## Webmessenger

Mithilfe eines Portals bzw. Webmessenger erhält ein Kommunikationspartner über eine sichere Internetverbindung Zugang zu einem E-Mail-Client. Über den von ALDI Nord zur Verfügung gestellten E-Mail Client hat der Kommunikationspartner die Möglichkeit, gesicherte E-Mails an ALDI Mitarbeiter zu versenden und zu empfangen.

Im Folgenden werden nochmals die Abläufe der gesicherten Kommunikation mit ALDI Nord dargestellt. Für die optimale Nutzung der gesicherten E-Mail Kommunikation empfehlen wir die Variante 1.

## 1. Variante:

**Sie haben bisher noch keinen gesicherten E-Mail-Kontakt mit ALDI Nord (auch keinen Webmessenger Zugang) und möchten zukünftig die verschlüsselte E-Mail-Kommunikation mit ALDI Nord einrichten (Schlüsselaustausch durch Publikation des öffentlichen Schlüssels auf dem Keyserver des Zertifikatsdiensteanbieters/Trustcenters).**

| | |
|---|---|
| **1** | **Beantragen** Sie ein persönliches S/MIME-E-Mail-Zertifikat von einem der Trustcenter aus der Übersicht im Anhang (publizieren Sie Ihren öffentlichen Schlüssel auf dem Keyserver des Trustcenters) (vgl. Anleitung Kap. 2.1 u. 2.2) |
| **2** | **Zuweisung** des Zertifikats zum persönlichen E-Mail-Konto in den Optionen der von Ihnen eingesetzten E-Mail-Software (vgl. Anleitung Kap. 2.4) |
| **3** | **ALDI Nord** fragt die Keyserver der im Anhang aufgezählten Trustcenter ab und nutzt Ihren öffentlichen Schlüssel (keine Aktion von Ihnen notwendig) |
| **4** | **Erhalt** einer verschlüsselten E-Mail von dem ALDI Nord Kommunikationspartner. Die E-Mail enthält das Zertifikat des ALDI Kommunikationspartners und das Stammzertifikat von ALDI Nord |
| **5** | **Anlegen** eines Kontakts für den ALDI Nord Kommunikations-partner im E-Mail-Programm und Zuweisen des entsprechenden Zertifikats zum angelegten Kontakt (vgl. Anleitung Kap. 2.5) |
| **6** | **Auswählen** der Verschlüsselungsoption S/MIME beim Verfassen einer E-Mail an den ALDI Kommunikationspartner (vgl. Anleitung Kap. 2.4) |

## 2. Variante:

**Sie haben von einem ALDI Kommunikationspartner einen Webmessenger Zugang erhalten und können hierüber gesicherte E-Mails an ALDI Kommunikationspartner versenden.**

**Unterstützter/s Zertifikatsdiensteanbieter/Trustcenter:**

| | |
|---|---|
| Swiss Sign | https://www.swisssign.com/ |
| Produkt: | Personal ID Silver |
| Hinweis: | Die Zertifikate sind auch außerhalb der Schweiz gültig. |
| Vertraute Stammzertifikate sind u.a.: | SwissSign Gold CA<br>SwissSign Gold CA G2<br>SwissSign Gold Root CA<br>SwissSign Gold Personal CA G3<br>SwissSign Silver CA G2<br>SwissSign Silver Root CA<br>SwissSign Silver Personal CA G3 |

**ALDI Nord Stammzertifikate und Prüfsummen**

1. ALDI Nord
   S/MIME Stammzertifikat
   Gültig ab 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 Stammzertifikat
   Gültig bis 06.01.2016

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