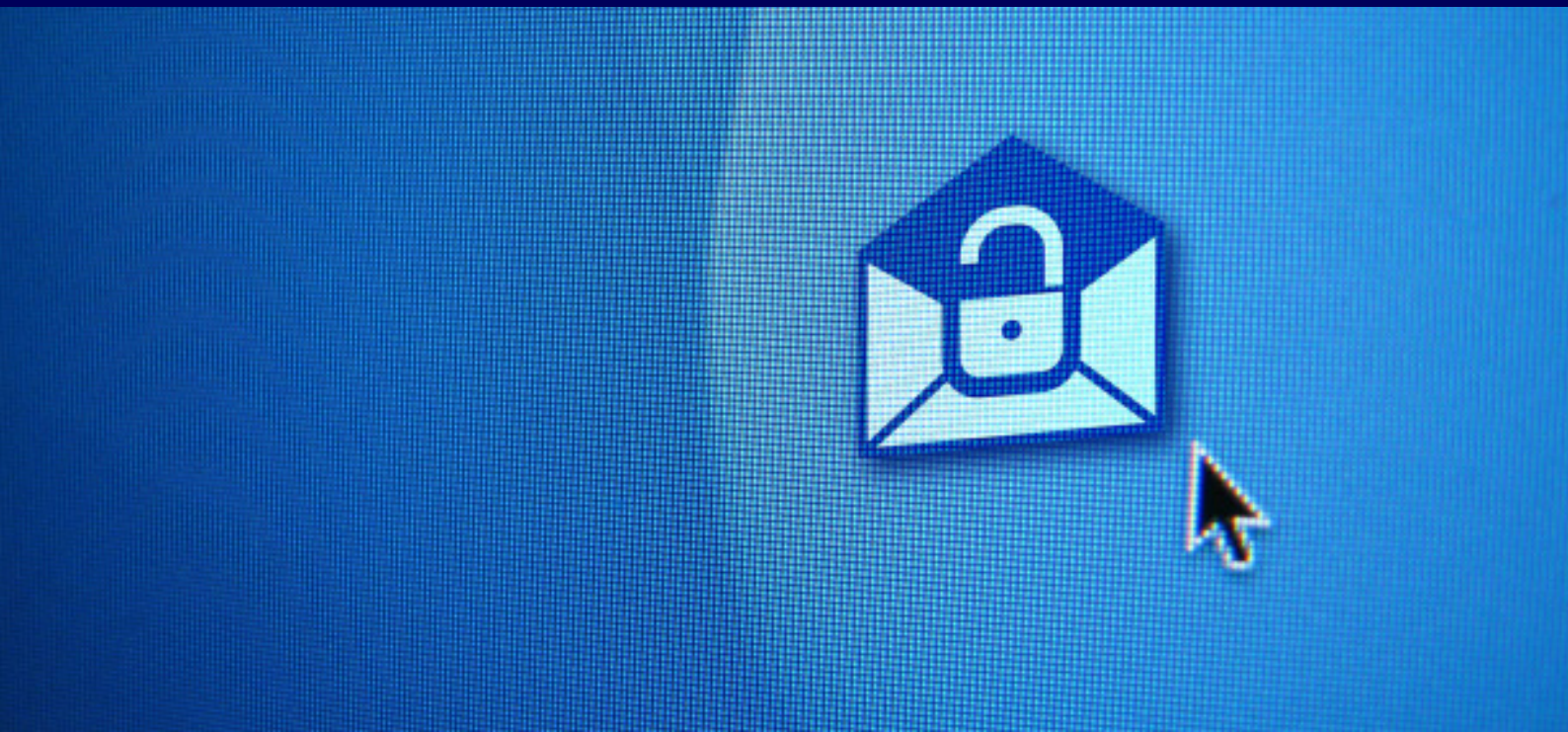
Informationen zur sicheren E-Mail-Kommunikation

Unternehmensgruppe ALDI SÜD



Sichere E-Mail-Kommunikation

Vorwort

E-Mail ist heute für Unternehmen ein häufig eingesetztes Kommunikationsmittel, das zum Austausch von Informationen verwendet wird. Auch die Unternehmensgruppe ALDI SÜD steht mit einer Vielzahl von Kommunikationspartnern per E-Mail in Kontakt.

Die Informationen, die über E-Mail ausgetauscht werden, sind dabei meist auch vertraulich, so dass 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 mit Bleistift beschriebenen 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 SÜD sichere Standardverfahren zum Austausch von verschlüsselten E-Mails.

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

Benutzerhinweis

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

Inhalt

Begriffserläuterungen

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 so genannten digitalen Zertifikat enthalten. Bevor ein gesicherter Austausch von Informationen in Form von verschlüsselten E-Mails stattfinden kann, müssen beide Kommunikationspartner über ein digitales Zertifikat verfügen.

Digitale Zertifikate

Mit einem digitalen Zertifikat kann sichergestellt werden, dass nur der vom Absender adressierte Empfänger einer E-Mail die darin enthaltenen Informationen in einer lesbaren Form erhält. Ein solches Zertifikat, auch Benutzerzertifikat genannt, wird für eine E-Mail-Adresse ausgestellt. Das Zertifikat ist eine digitale Beglaubigung der Identität des Absenders und wird zum einen als eine sogenannte digitale Signatur von E-Mails verwendet. Zum anderen können damit E-Mails verschlüsselt werden.

Durch die Beglaubigung kann die zertifizierte E-Mail-Adresse über einen definierten Zeitraum als gültig angesehen werden. Die Gültigkeitsdauer eines digitalen Zertifikats beträgt in der Regel zwischen einem und fünf Jahren.

Öffentliche und private Schlüssel

Ein Benutzerzertifikat 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 Benutzerzertifikats 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.

Begriffserläuterungen

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, so dass 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 SÜD akzeptiert ausschließlich das S/MIME-Verfahren zur E-Mail-Verschlüsselung.

Zertifikatsdiensteanbieter

Ein Zertifikatsdiensteanbieter (auch Trust-Center 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 E-Mail-Zertifikat besitzen, können Sie dieses bei einem Zertifikatsdiensteanbieter beantragen. Eine Übersicht von Anbietern, der die Unternehmensgruppe ALDI SÜD vertraut, finden Sie im Anhang. Der Zertifikatsservice der Anbieter ist in der Regel kostenpflichtig.

Stammzertifikat

Zusätzlich zu dem Benutzerzertifikat wird bei der E-Mail-Kommunikation mit der Unternehmensgruppe ALDI SÜD auch ein so genanntes Stammzertifikat benötigt. Mit diesem kann der Vertrauensstatus der Benutzerzertifikate der Unternehmensgruppe ALDI SÜD überprüft werden. Das bedeutet, dass das von Ihnen eingesetzte System überprüfen kann, ob das Benutzerzertifikat wirklich von der Unternehmensgruppe ALDI SÜD stammt und ob es noch gültig ist.

Begriffserläuterungen

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 SÜD übermitteln

Wenn Sie Ihr persönliches Benutzerzertifikat von einem der Zertifikatsdiensteanbieter aus der Liste im Anhang erhalten haben, brauchen Sie Ihrem Kommunikationspartner in der Unternehmensgruppe ALDI SÜD für die Bereitstellung des öffentlichen Schlüssels nur einmalig eine signierte E-Mail zusenden. Diesen Vorgang müssen Sie erst wiederholen, wenn sich Ihr Benutzerzertifikat geändert hat, z.B. aufgrund des Wechsels Ihres Zertifikatsanbieters.

Zertifikate von der Unternehmensgruppe ALDI SÜD erhalten

Das jeweilige Benutzerzertifikat erhalten Sie durch eine signierte E-Mail von Ihrem Kommunikationspartner in der Unternehmensgruppe ALDI SÜD. Das Stammzertifikat muss für die Überprüfung der Benutzerzertifikate der Unternehmensgruppe ALDI SÜD auf Ihrem Endgerät (z. B. PC) einmalig importiert werden. Das Benutzerzertifikat muss dem entsprechenden Kontakt in dem eingesetzten E-Mail-Programm zugeordnet werden.

Die Gültigkeit der Benutzerzertifikate der Unternehmensgruppe ALDI SÜD beträgt drei Jahre.

Das Stammzertifikat der Unternehmensgruppe ALDI SÜD kann unter der Adresse **www.aldi-sued.com/cert/** heruntergeladen werden.

Anleitung für die sichere E-Mail-Kommunikation

1. **Import** des Stammzertifikats der Unternehmensgruppe ALDI SÜD.

   Das Stammzertifikat kann unter der Adresse **www.aldi-sued.com/cert** heruntergeladen werden.

2. **Anfordern** eines persönlichen S/MIME-E-Mail-Zertifikats von einem der Zertifikatsdiensteanbieter aus der Übersicht im Anhang und zuweisen zum persönlichen E-Mail-Konto in den entsprechenden Optionen der eingesetzten E-Mail-Software.

3. **Senden** einer signierten E-Mail an den Kommunikationspartner in der Unternehmensgruppe ALDI SÜD.

4. **Erhalt** einer signierten E-Mail von dem Kommunikationspartner in der Unternehmensgruppe ALDI SÜD. Die signierte E-Mail enthält das Benutzerzertifikat des Kommunikationspartners.

5. **Anlegen** eines Kontakts für den Kommunikationspartner in der Unternehmensgruppe ALDI SÜD im eingesetzten E-Mail-Programm und zuweisen des entsprechenden Benutzerzertifikats zum angelegten Kontakt.

6. **Auswählen** der Verschlüsselungsoption S/MIME beim Verfassen einer E-Mail an den Kommunikationspartner in der Unternehmensgruppe ALDI SÜD.

Anhang

Liste unterstützter Zertifikatsdiensteanbieter

Comodo www.comodo.com
Produkt: Secure E-mail Certificate

Vertraute Stammzertifikate: AddTrust External CA Root
UTN-USERFIRST-Client Authentication and Email

Entrust www.entrust.com
Produkt: Secure E-mail Certificate
Vertraute Stammzertifikate: Entrust.net Certificate Authority (2048)

GeoTrust www.globalsign.com
Produkt: Small & Medium Businesses /
Secure E-mail Certificate
Enterprise / S/MIME
Vertraute Stammzertifikate: GlobalSign Primary Class 1 CA
GlobalSign Primary Class 2 CA

SwissSign www.swisssign.com
Produkt: Personal Silver ID
Personal Gold ID

Vertraute Stammzertifikate: SwissSign Personal Silver CA 2008 - G2
SwissSign Personal Gold CA 2008 - G2

Checksum (fingerprint) S/MIME root certificate

MailGateway ALDI-HOFER CA

SHA1:	03BD AB3C	A1EE 9FDC	9EC4 52A9	DE3D 0C08	B1A5 39B3
MD5:	0D9C 43BF	29BF 8607	E2E6 8276	3489 CF85	

Mülheim an der Ruhr, April 2018