## Przedmowa

Poczta elektroniczna jest jednym z najczęściej stosowanych środków komunikacji służących do wymiany informacji w szczególności w firmach.

Również ALDI Nord kontaktuje się ze swoimi partnerami biznesowymi za pomocą poczty elektronicznej.
Informacje wymieniane za pomocą wiadomości e-mail są najczęściej poufne, dlatego muszą podlegać szczególnej ochronie przed nieuprawnionym dostępem i ingerencją w ich treść. Bez odrębnego zabezpieczenia transmisja danych pomiędzy nadawcą a odbiorcą odbywająca się za pomocą Internetu jest całkowicie niechroniona, a zabezpieczenie przed wyciekiem danych porównywalne z wysłaniem wiadomości pocztówką.
W celu zapewnienia skutecznej ochrony korespondencji elektronicznej niezbędne jest wdrożenie dodatkowych działań zabezpieczających.
W celu zachowania poufności informacji zawartych w przesyłanych e-mailach grupa ALDI Nord stosuje standardową metodę szyfrowania wiadomości.

Niniejsza instrukcja dostarcza wskazówek jak zapewnić bezpieczną komunikację drogą elektroniczną.

Poniżej wyjaśnione zostały istotne pojęcia dotyczące szyfrowania wiadomości e-mail oraz przedstawiono podstawowe kroki konfiguracji i ustawienia bezpiecznego systemu komunikacyjnego.

Następnie przedstawione zostały dwa warianty wysyłania szyfrowanych wiadomości. Do dokumentów została dołączona również krótka instrukcja.

W przypadku pytań dotyczących wdrażanych przez firmę rozwiązań co do szyfrowania wiadomości, należy zwrócić się do odpowiedniej osoby kontaktowej ds. technicznych.

## Szyfrowanie

W celu zachowania poufności komunikacji poczty elektronicznej, wiadomości e-mail muszą być zaszyfrowane.
Niezbędne informacje potrzebne do szyfrowania i odszyfrowania poczty elektronicznej zawarte są w tak zwanym certyfikacie wraz z kluczem publicznym do szyfrowania (dla wszystkich stron prowadzących korespondencję) oraz prywatnym kluczem do odszyfrowania (tylko dla właściciela). Tak więc zanim będzie mogła nastąpić bezpieczna wymiana informacji w formie zaszyfrowanej wiadomości e-mail, obydwaj partnerzy muszą dysponować publicznym kluczem swojego rozmówcy.

## Publiczne i prywatne klucze

Certyfikat składa się z dwóch części: publicznego i prywatnego klucza.
Prywatny klucz jest stosowany do podpisywania i odszyfrowywania poczty elektronicznej a jego ujawnianie jest zabronione.
Publiczny klucz musi być udostępniony odbiorcy wiadomości, aby ten mógł zweryfikować podpis wiadomości e-mail oraz wysłać zaszyfrowaną wiadomość e-mail do właściciela prywatnego klucza.

Przed pierwszym zaszyfrowaniem wiadomości e-mail nadawca musi otrzymać od odbiorcy jego publiczny klucz będący częścią certyfikatu. Wymiana ta następuje z reguły poprzez wysyłkę sygnowanego podpisem e-maila, z którego odbiorca pobiera publiczny klucz. Dopiero wówczas nadawca może szyfrować wiadomość za pomocą publicznego klucza odbiorcy.
Po otrzymaniu zaszyfrowanej wiadomości odbiorca może odszyfrować ją używając swojego prywatnego klucza. Procesy te są przeprowadzane automatycznie i wykonywane w tle przez większość programów pocztowych.

## Podpisy

Aby program pocztowy automatycznie rozpoznał zaufany adres poczty elektronicznej, potrzebny jest podpis cyfrowy. Można nim jednoznacznie zidentyfikować nadawcę wiadomości e-mail.
Poza tym gwarantuje on, że treść wiadomości pozostała nienaruszona, bowiem w przypadku modyfikacji zawartości podpis cyfrowy traci swoją ważność – podobnie jak złamanie pieczęci listu.
Dlatego przy podpisywaniu e-maila dołączany jest do niego zawsze publiczny klucz certyfikatu, aby odbiorca mógł sprawdzić autentyczność i autentyczność wiadomości
e-mail.
Poprzez złożenie podpisu elektronicznego treść wiadomości zostaje zabezpieczona w taki sposób, że odbiorca widzi wszelkie zmiany wprowadzone po podpisaniu e-maila. Jednak nadal istnieje możliwość ich jawnego odczytania.
Aby zagwarantować poufność wiadomości, e-mail musi zostać dodatkowo zaszyfrowany. Najlepszą metodą zabezpieczenia poufności wiadomości e-mail jest kombinacja podpisu elektronicznego z zaszyfrowaniem wiadomości.

## S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) to stosowana na całym świecie standardowa metoda zabezpieczająca drogą certyfikacji wymianę informacji za pomocą poczty elektronicznej .Niezbędne elementy dla S/MIME są już zintegrowane w większości nowoczesnych programów poczty elektronicznej, dzięki czemu zagwarantowana jest prosta i przejrzysta obsługa. Oznacza to, że e-maile są automatycznie szyfrowane poprzez aktywowanie odpowiedniej opcji w programie poczty elektronicznej przed wysyłką a przy odbiorze automatycznie odszyfrowywane.

Grupa przedsiębiorstw ALDI Nord akceptuje wyłącznie metodę S/MIME do szyfrowania wiadomości poczty elektronicznej.

## Dostawca certyfikatu/Trustcenter

Dostawca certyfikatu (zwany także Trustcenter) jest organizacją, która wydaje cyfrowe certyfikaty użytkownika oraz jest odpowiedzialna za ich przygotowanie, przydzielenie i zabezpieczenie integralności.
Jeśli systemem poczty elektronicznej przystosowanym jest już do S/MIME, ale użytkownik nie posiada jeszcze własnego certyfikatu, złożyć wniosek o jego wydanie u dostawcy certyfikatu. Spis zaufanych dla ALDI Nord dostawców certyfikatów została załączona do niniejszego dokumentu w formie aneksu.

## Główny certyfikat

W celu nawiązania kontaktu drogą elektroniczną z grupą ALDI Nord poza certyfikatem danego użytkownika potrzebny jest także tak zwany certyfikat główny. Certyfikat główny umożliwia zweryfikowanie statusu zaufania pozostałych certyfikatów ALDI Nord.
Oznacza to, że system z którego korzysta użytkownik może sprawdzić, czy certyfikat rzeczywiście pochodzi od grupy ALDI Nord i czy jest jeszcze ważny.

## Wymiana certyfikatu

Wymiana certyfikatu pomiędzy nadawcą a odbiorcą musi zostać przeprowadzona przed pierwszym szyfrowaniem i jest potrzebna ponownie dopiero wówczas, gdy jeden z wymienionych certyfikatów straci swoją ważność.

Dostarczanie certyfikatu do grupy przedsiębiorstw ALDI Nord:
Po otrzymaniu osobistego certyfikatu od jednego z dostawców certyfikatów/Trustcenter z listy znajdującej się w aneksie i zamieszczeniu klucza publicznego na serwerze kluczy (porównaj instrukcję rozdz. 2.1) pobieranie klucza publicznego z serwera będzie następować automatycznie.Alternatywą dla zamieszczenia klucza publicznego na serwerze kluczy dostawcy certyfikatów/Trustcenter jest udostępnienie go poprzez portal certyfikatów ALDI (www.aldi-nord.de/certportal).

W przypadku zmiany certyfikatu użytkownika należy powtórzyć powyższy proces

Otrzymanie certyfikatu od grupy przedsiębiorstw ALDI Nord:
Określony certyfikat użytkownika zostaje przesyłany automatycznie z każdą otrzymaną od ALDI Nord zaszyfrowaną wiadomością e-mail. Możliwe jest również pobranie certyfikatów osób kontaktowych firmy ALDI poprzez portal certyfikatów ALDI (www.aldi-nord.de/certportal) podając dokładny adres poczty elektronicznej konkretnej osoby.
Główny certyfikat otrzymywany automatycznie z zaszyfrowaną wiadomością od ALDI Nord musi zostać jednorazowo zaimportowana na terminal (np. komputer osobisty) celem weryfikacji certyfikatów.
Certyfikat użytkownika należy przyporządkować do odpowiedniego kontaktu ze skrzynki nadawczej programu poczty elektronicznej (porównaj instrukcję rozdz. 2.5).
Główny certyfikat grupy ALDI Nord można pobrać poprzez portal certyfikatów ALDI (www.aldi-nord.de/certportal) jak i pod adresem www.aldi-nord.de/cert/ lub też otrzymać automatycznie z każdą zaszyfrowaną wiadomością e-mail (jako załącznik) (porównaj instrukcję rozdz. 4).

## Webmessenger

Za pomocą portalu Webmessenger partner biznesowy grupy ALDI Nord otrzymuje bezpieczny dostęp do programu E-Mail-Client. Poprzez udostępniony przez ALDI Nord program E-Mail-Client użytkownik ma możliwość wysyłania do i odbierania od ALDI Nord zabezpieczonych wiadomości e-mail.

Poniżej przedstawiono jeszcze raz sposoby prowadzenia bezpiecznej korespondencji z ALDI Nord. W celu optymalnego korzystania z bezpiecznej wymiany informacji za pomocą poczty elektronicznej zalecany jest wariant 1.

## Wariant 1:

**Użytkownik (partner biznesowy ALDI) nie kontaktował się dotychczas z ALDI Nord za pomocą szyfrowanej poczty elektronicznej (nie korzystał również z dostępu przez Webmessenger) i zamierza rozpocząć korzystanie z korespondencji poufnej (wymiana szyfrów przez publikację publicznego klucza na serwerze kluczy dostawcy certyfikatów/Trustcenter).**

**Krok 1** **Złożenie wniosku** osobistego certyfikatu poczty elektronicznej S/MIME od Trustcenter z listy znajdującej się w aneksie (udostępnienie swojego klucza publicznego na serwerze kluczy Trustcenter) (porównaj instrukcję w rozdziale 2.1 i 2.2)

**Krok 2** **Przypisanie certyfikatu** do osobistego konta poczty elektronicznej w ustawieniach programu pocztowego wykorzystywanego przez partnera biznesowego ALDI Nord (porównaj instrukcję rozdz. 2.4)

**Krok 3** **ALDI Nord** wysyła zapytanie do serwera kluczy wymienionego w aneksie Trustcenter i wykorzystuje publiczny klucz użytkownika (nie wymaga działania ze strony partnera ALDI)

**Krok 4** **Otrzymanie** zaszyfrowanej wiadomości e-mail od osoby kontaktowej z ALDI Nord. E-mail zawiera certyfikat poczty osoby kontaktowej ALDI oraz certyfikat główny ALDI Nord

**Krok 5** **Utworzenie** kontaktu dla osoby kontaktowej z ALDI Nord w programie poczty elektronicznej użytkownika oraz przydzielenie odpowiedniego certyfikatu do utworzonego kontaktu (porównaj instrukcję rozdz. 2.5)

**Krok 6** **Wybór** opcji szyfrowania S/MIME przy redagowaniu wiadomości e-mail do osoby kontaktowej z ALDI (porównaj instrukcję rozdz. 2.4)

## Wariant 2:

**Partner biznesowy ALDI otrzymał dostęp do Webmessenger i może przesyłać zabezpieczone wiadomości e-mail do osoby kontaktowej w ALDI.**

**Lista obsługiwanych dostawców certyfikatów/Trustcenter:**

| | |
|---|---|
| Swiss Sign | https://www.swisssign.com/ |
| Produkt: | Personal ID Silver/ Osobisty ID srebrny |
| Wskazówka: | Certyfikaty obowiązują także poza Szwajcarią.dniesienie pod hasłem „Do nabycia poza USA“ na stronie Symantec można zignorować. |
| Zaufane główne Certyfikaty to między innymi: | 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 |

**Certyfikat główny i sumy kontrolne dla ALDI Polska sp. z o.o.**

**1. ALDI Polska Sp. z o.o.**
**S/MIME certyfikat główny**
**Ważny od 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 Polska Sp. z o.o.**
**S/MIME certyfikat główny**
**Ważny do 06.01.2016**

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