Preamble

In today's business, email is a common medium which is used by companies to exchange information.

ALDI Nord, too, stays in contact with a lot of communication partners via email.
The information that is exchanged via email is often confidential, so there is a special need to protect them from manipulation and unauthorized access. Without a separate protection, the data transfer through the internet is completely unprotected and comparable to sending a postcard.
Because of that, additional security measures to protect the communication effectively are absolutely necessary.
To shelter confidential information in emails, ALDI Nord uses safe standard procedures for the exchange of encrypted email.

With this document, ALDI Nord wants to provide you all necessary information to set up a secure communication between yourself and ALDI Nord.

In the following, the relevant terms concerning email encryption and the basic steps setting up and configuring encrypted email will be explained.

Afterwards, two variants to initialize encrypted communication with ALDI Nord will be presented. For this, you will find a short tutorial at the end of this document.

If you have questions related to the email encryption used in your company, please contact the technical support at your company.

Encryption

To maintain confidentiality in email communication, emails have to be encrypted.
The required information to encrypt and decrypt emails is contained in a so called "digital certificate", which contains a public key (for all communication partners) for encryption and a private key (only for the owner) for decryption. Thus both communication partners have to hold the public key of the other before encrypted exchange of emails can be accomplished.

Public and private keys

A user certificate consists of two parts: a public key and a private key. The private key is used to sign and decrypt emails and must never be published.
The public key has to be provided to the communication partner to let him check the signature of an email and send encrypted emails to the owner of the public key.

Before encrypting emails for the first time, the sender has to receive the public key of the recipient as a part of the recipient's user certificate. This exchange usually takes place by sending a signed email so that the recipient can extract the public key from it. From this point, the sender can encrypt his message with the public key of the recipient.
Once the encrypted email has been received, the recipient can decrypt it with his/her private key. This process is carried out automatically by most email programs.

Signatures

To verify the authenticity of an email address automatically, a digital signature is required. This allows the sender of an e-mail to be identified clearly. A digital signature also guarantees the integrity of the email, because the signature – comparable to an unsealed envelope – is destroyed if the data is changed later.
So, when signing an e-mail, the public key of the certificate is always attached so that the recipient can check the authenticity and integrity of the email.
Once you have signed an email, no one can change the information contained in it without the recipient's knowledge. The information is however still freely readable. To ensure confidentiality when exchanging information, the email must be additionally encrypted. The most secure way to exchange emails is to combine a signature with encryption.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard procedure used world-wide for exchanging information securely via email using certificates.
The components required for S/MIME are already integrated into most modern email programs to ensure simple and transparent use. This means that, by activating the relevant option in the email program, emails are automatically encrypted before sending and automatically decrypted upon receipt.

The ALDI Nord group accepts only the S/MIME procedure for encrypting emails.

Certification Authority / Trust Center

A Certification Authority (also known as a TrustCenter) is an organisation that issues digital user certificates and is responsible for their provision, assignment and integrity.
If you have an S/MIME compatible email system but do not have your own email certificate yet, you can request this from a Certification Authority. You can find an overview of providers trusted by the ALDI Nord group attached.

Root certificate

In addition to the user certificate, a so-called root certificate is also required to communicate with the ALDI Nord group via email. You can check the confidentiality of the ALDI Nord group user certificate by using this root certificate.
This means that the system you use can check if the user certificate is really from the ALDI Nord group and if it is still valid.

Exchange of certificates

The exchange of certificates between the communication partners must only be carried out once before the first encryption and is only required again if one of the exchanged certificates becomes invalid.

Transmitting a certificate to the ALDI Nord group:
If you have received your personal user certificate from one of the Certification Authorities / Trust Centers from the list attached and have stored your public key on the Certification Authority / Trust Center keyserver (cf. Instructions section 2.1), your ALDI Nord contact partner will query the Certification Authority / Trust Center keyserver and thus receive your public key automatically.
If you have not published your public key on the Certification Authority / Trust Center keyserver, there is the possibility to make your public key available using the ALDI certificate portal (www.aldi-nord.de/certportal).

If your user certificate has been changed, e.g. because you have changed your Certification Authority, you must repeat the process.

Receiving certificates from the ALDI Nord group:
You will automatically receive the respective user certificate with the email from your ALDI Nord group communication partner. Furthermore you can download the certificates of your contacts using the ALDI certificate portal. For that, you have to know the e-mail address of the recipient. The root certificate, which you will also automatically receive with an encrypted email from your ALDI Nord communication partner, must be imported once to check the ALDI Nord group user certificate on your terminal device (e.g. computer).
The user certificate has to be matched with the relevant contact in the email program used (cf. Instructions section 2.5)
The ALDI Nord group root certificate can either be downloaded via the ALDI certificate portal (www.aldi-nord.de/certportal), automatically with the email from your ALDI Nord communication partner, under the address www.aldi-nord.de/cert/, or you can receive it automatically as an e-mail attachment from your ALDI Nord communication partner
(cf. Instructions section 4).

Web messenger

With the help of a portal or web messenger, a communication partner can gain access to an email client via a secure internet connection. The email client provided by ALDI Nord allows the communication partner to send and receive emails to and from ALDI employees.

The following explains again the steps required for encrypted communication with ALDI Nord. For optimal use of secure communication, we recommend option 1.

Option 1:

You have not yet had contact with ALDI Nord via e-mail (and also no web messenger access) and would like to set up encrypted e-mail communication with ALDI Nord in the future (exchanging keys by publishing the public key on the Certification Authority / Trust Center keyserver).

1 **Request** a personal S/MIME e-mail certificate from one of the TrustCenters in the overview attached (publish your public key on the TrustCenter keyserver) (cf. Instructions sections 2.1 and 2.2)

2 **Assign** the certificate to the personal email account in the options of the email software you use (cf. Instructions section 2.4)

3 **ALDI Nord** queries the keyservers of the TrustCenters attached and stores your public key (no further action is required)

4 **Receive** an encrypted email from your ALDI Nord communication partner. The email contains the ALDI communication partner's user certificate and the root certificate

5 **Create** your ALDI Nord communication partner as a contact in the e-mail program and assign the relevant user certificate to the contact created (cf. Instructions section 2.5)

6 **Select** the S/MIME encryption option when composing an email to the ALDI communication partner (cf. Instructions section 2.4)

Option 2:

You have received access to the web messenger and you are herewith able to exchange save e-mail traffic with ALDI communication partners.

List of supported Certification Authorities / TrustCenters:

SwissSign	www.swisssign.com
Product:	Personal ID Silver
Note:	These certificates can also be used outside of Switzerland.

Trustedroot certificates includes i.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

ALDI Nord root certificate and thumbprint

1. ALDI Nord
   S/MIME root certificate
   Valid from 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 root certificate
   Valid till 06.01.2016

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