Préambule

La messagerie électronique est aujourd'hui un moyen de communication fréquemment utilisé par les entreprises pour échanger des informations.

Le groupe commercial ALDI NORD demeure, lui aussi, en contact avec de nombreux partenaires de communication grâce à la messagerie électronique.
Or, les informations échangées par e-mail sont la plupart du temps confidentielles si bien qu'elles doivent être protégées des manipulations et des accès externes. Sans protection particulière, l'échange de données sur Internet entre expéditeurs et destinataires est totalement exposé et comparable à l'envoi d'une carte postale.
Par conséquent, pour garantir la protection optimale des échanges de messages électroniques, des mesures de sécurité supplémentaires sont impératives.
Afin de protéger les informations confidentielles contenues dans les messages électroniques, le groupe commercial ALDI Nord utilise des protocoles standards sécurisés pour l'échange de messages électroniques chiffrés.

À travers ce document, le groupe commercial ALDI Nord entend mettre à votre disposition toutes les informations nécessaires pour vous permettre d'établir un mode de communication sécurisé entre vous et le groupe.

Les termes relatifs au chiffrement des e-mails, ainsi que les principales étapes concernant la configuration et l'installation d'un système de communication sécurisé, sont expliqués dans ce qui suit.

Deux options permettant de mettre en œuvre un système de communication chiffrée avec ALDI Nord sont ensuite présentées. Vous trouverez, à la fin de ce document, une brève présentation des procédures correspondantes.

Pour toute question concernant le chiffrement des messages électroniques en relation avec la solution de messagerie utilisée dans votre entreprise, veuillez contacter le responsable technique de votre entreprise.

Chiffrement

Pour préserver la confidentialité d'une communication électronique, les e-mails doivent être chiffrés.
Les informations nécessaires au chiffrement et au déchiffrement des e-mails sont contenues dans un « certificat numérique » qui contient la clé publique (pour tous les partenaires de communication) pour le chiffrement et la clé privée (uniquement pour le propriétaire) pour le déchiffrement. Avant qu'un échange d'informations sécurisé puisse être effectué sous la forme d'e-mails chiffrés, les deux partenaires de communication doivent disposer de la clé publique de l'autre.

Clé publique et clé privée

Un certificat utilisateur comprend deux parties : une clé publique et une clé privée.
La clé privée est utilisée pour la signature et le déchiffrement des e-mails et ne doit jamais être publiée.
La clé publique doit être mise à la disposition du partenaire de communication afin qu'il puisse vérifier la signature d'un message électronique et envoyer des e-mails chiffrés au détenteur de la clé.

Avant le premier chiffrement de messages électroniques, l'expéditeur doit avoir reçu la clé publique comme partie du certificat utilisateur du destinataire de l'e-mail. Cet échange se fait généralement par le biais de l'envoi d'un e-mail signé à partir duquel la clé publique peut être extraite par le destinataire. L'expéditeur peut ensuite chiffrer le message électronique à l'aide de la clé publique du destinataire.
À réception de l'e-mail chiffré, le destinataire peut le décoder grâce à sa clé privée. Ces processus sont exécutés automatiquement par la plupart des clients de messagerie.

Signatures

Pour que l'authenticité d'une adresse électronique puisse être automatiquement vérifiée, une signature numérique est nécessaire. Cette signature permet d'identifier formellement l'expéditeur d'un e-mail.
L'intégrité de l'e-mail est en outre garantie, la signature numérique étant détruite avec la modification ultérieure des données, telle une lettre décachetée.
C'est pour cette raison que, lors de la signature d'un e-mail, la clé publique du certificat est toujours ajoutée au message afin que le destinataire puisse vérifier l'authenticité et l'intégrité de l'e-mail.
Grâce à la signature d'un e-mail, les informations contenues dans le message ne peuvent être modifiées sans que le destinataire ne s'en aperçoive. Mais elles restent lisibles par n'importe qui. Pour garantir la confidentialité des informations, le message électronique doit en outre être chiffré. En matière d'échange d'e-mails, le procédé le plus sûr consiste à combiner signature et chiffrement.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) est un protocole standard utilisé au niveau international pour l'échange sécurisé d'informations par e-mail à l'aide de certificats. Les composantes nécessaires au fonctionnement de S/MIME sont déjà intégrées à la plupart des clients de messagerie modernes de façon à garantir une utilisation simple et transparente. Cela signifie que les e-mails sont automatiquement chiffrés avant leur envoi et automatiquement déchiffrés lors de leur réception grâce à l'activation de l'option correspondante dans le client de messagerie.

Le groupe ALDI Nord accepte uniquement le protocole S/MIME pour le chiffrement des messages électroniques.

Fournisseurs de services de certification / Centres de gestion de la confidentialité

Un fournisseur de services de certification (également appelé centre de gestion de la confidentialité) est une organisation qui délivre des certificats numériques et qui est responsable de leur préparation, de leur attribution et de la garantie de leur intégrité.
Si vous disposez d'un système de messagerie électronique compatible avec S/MIME, mais que vous n'avez pas encore de certificat de messagerie, vous pouvez en demander un auprès d'un fournisseur de services de certification. Vous trouverez en annexe un aperçu des fournisseurs auxquels le groupe ALDI Nord fait confiance.

Certificat racine

Outre le certificat utilisateur, un certificat racine est également nécessaire pour communiquer par e-mail avec le groupe ALDI Nord. Ce certificat permet de vérifier le niveau de confiance des certificats utilisateur du groupe ALDI Nord.
Cela signifie que le système que vous utilisez peut vérifier si le certificat utilisateur provient réellement du groupe ALDI Nord ou s'il est encore valide.

Échange de certificats

L'échange de certificats entre les partenaires de communication ne doit être effectué qu'une seule fois avant le premier chiffrement et s'avère par la suite une nouvelle fois nécessaire si l'un des certificats échangés n'est plus valide.

Transmission du certificat au groupe ALDI Nord :
Une fois que vous avez reçu votre certificat personnel d'un fournisseur de services de certification ou d'un centre de gestion de la confidentialité figurant sur la liste présentée en annexe et que vous avez enregistré votre clé publique sur le serveur de clés du fournisseur de services de certification ou du centre de gestion de la confidentialité (voir manuel, chapitre 2.1), votre interlocuteur chez ALDI Nord interroge le serveur de clés et reçoit automatiquement sa clé publique.
Si vous n'avez pas publié votre clé publique sur le serveur de clés du fournisseur de services de certification ou du centre de gestion de la

confidentialité, vous pouvez l'accéder depuis le portail des certificats ALDI (www.aldi-nord.de/certportal).
Si votre certificat utilisateur a changé (par exemple du fait d'un changement de fournisseur), vous devez répéter ces opérations.

Réception du certificat du groupe ALDI Nord (voir manuel, chapitre 4) :
Vous recevez automatiquement le certificat utilisateur correspondant avec l'e-mail de votre interlocuteur au sein du groupe ALDI Nord. De plus, vous pouvez télécharger les certificats de vos personnes de contact au sein d'ALDI depuis le portail des certificats (www.aldi-nord.de/certportal) en introduisant l'adresse électronique exacte. Le certificat racine, qui vous est également transmis automatiquement avec l'e-mail de votre interlocuteur au sein du groupe ALDI Nord, doit être importé une seule fois sur votre équipement (PC, p. ex.) pour la vérification des certificats utilisateur du groupe ALDI Nord.
Le certificat utilisateur doit être associé au contact correspondant dans le client de messagerie utilisé (voir manuel, chapitre 2.5).
Le certificat racine du groupe ALDI Nord peut être soit téléchargé à partir du portail de certificats ALDI (www.aldi-nord.de/certportal) ou à l'adresse **www.aldi-nord.de/cert/**, soit reçu automatiquement par le biais de l'e-mail chiffré envoyé (en tant que pièce jointe) par votre partenaire de communication chez ALDI Nord (voir manuel, chapitre 4).

Client de messagerie instantanée

Grâce à un portail, ou plus exactement à un client de messagerie instantanée, un partenaire de communication dispose d'un accès sécurisé à un client de messagerie électronique. Le client de messagerie mis à disposition par ALDI Nord permet au partenaire de communication d'échanger des e-mails avec les collaborateurs d'ALDI.

Le fonctionnement des messages chiffrés échangés avec ALDI Nord est de nouveau présenté dans les pages suivantes. Pour mettre en place un mode de communication chiffrée optimal, nous vous recommandons l'option 1 lors de l'acquisition du certificat.

Option 1 :

Vous n'avez pas encore eu de contact sécurisé par e-mail avec ALDI Nord (et donc pas d'accès à un client de messagerie instantanée) et souhaitez mettre en place le chiffrement des messages électroniques pour vos échanges avec ALDI Nord (échange de clés en publiant la clé publique sur le serveur de clés du fournisseur de services de certification ou du centre de gestion de la confidentialité).

1	**Demandez** un certificat e-mail S/MIME personnel auprès d'un centre de gestion de la confidentialité figurant dans la liste en annexe (publiez votre clé publique sur le serveur de clés du centre de gestion de la confidentialité) (voir manuel, chapitres 2.1 et 2.2)
2	**Attribution du certificat** au compte personnel de courrier électronique dans les options du logiciel utilisé (voir manuel, chapitre 2.4)
3	**ALDI Nord** interroge le serveur de clés du centre de gestion de la confidentialité répertoriée en annexe et enregistre votre clé publique (ne nécessite aucune action de votre part)
4	**Réception** d'un e-mail chiffré de la part du partenaire de communication chez ALDI Nord. Cet e-mail contient le certificat utilisateur de votre partenaire de communication ALDI ainsi que le certificat racine d'ALDI Nord
5	**Création** d'un contact pour le partenaire de communication ALDI Nord dans le client de messagerie et attribution du certificat utilisateur correspondant au contact créé (voir manuel, chapitre 2.5)
6	**Sélection** du mode de chiffrement S/MIME lors de la rédaction d'un e-mail destiné au partenaire de communication ALDI (voir manuel, chapitre 2.4)

Option 2 :

Vous avez déjà reçu un accès à un client de messagerie instantanée par le biais d'un partenaire de communication ALDI et pouvez envoyer des e-mails chiffrés aux partenaires de communication ALDI par le biais de celui-ci.

Liste des fournisseurs de services de certification et centres de gestion de la confidentialité agréés :

SwissSign :	https://www.swisssign.com/
Produit :	Personal ID Silver
Remarque :	Les certificats sont également valables hors Suisse.

Les certificats racine de confiance
sont entre autres :
- 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

Certificats racine ALDI Nord et sommes de contrôle

1. ALDI Nord
   Certificat racine S/MIME
   Valable à partir du 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
   Certificat racine S/MIME
   Valable jusqu'au 06.01.2016

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