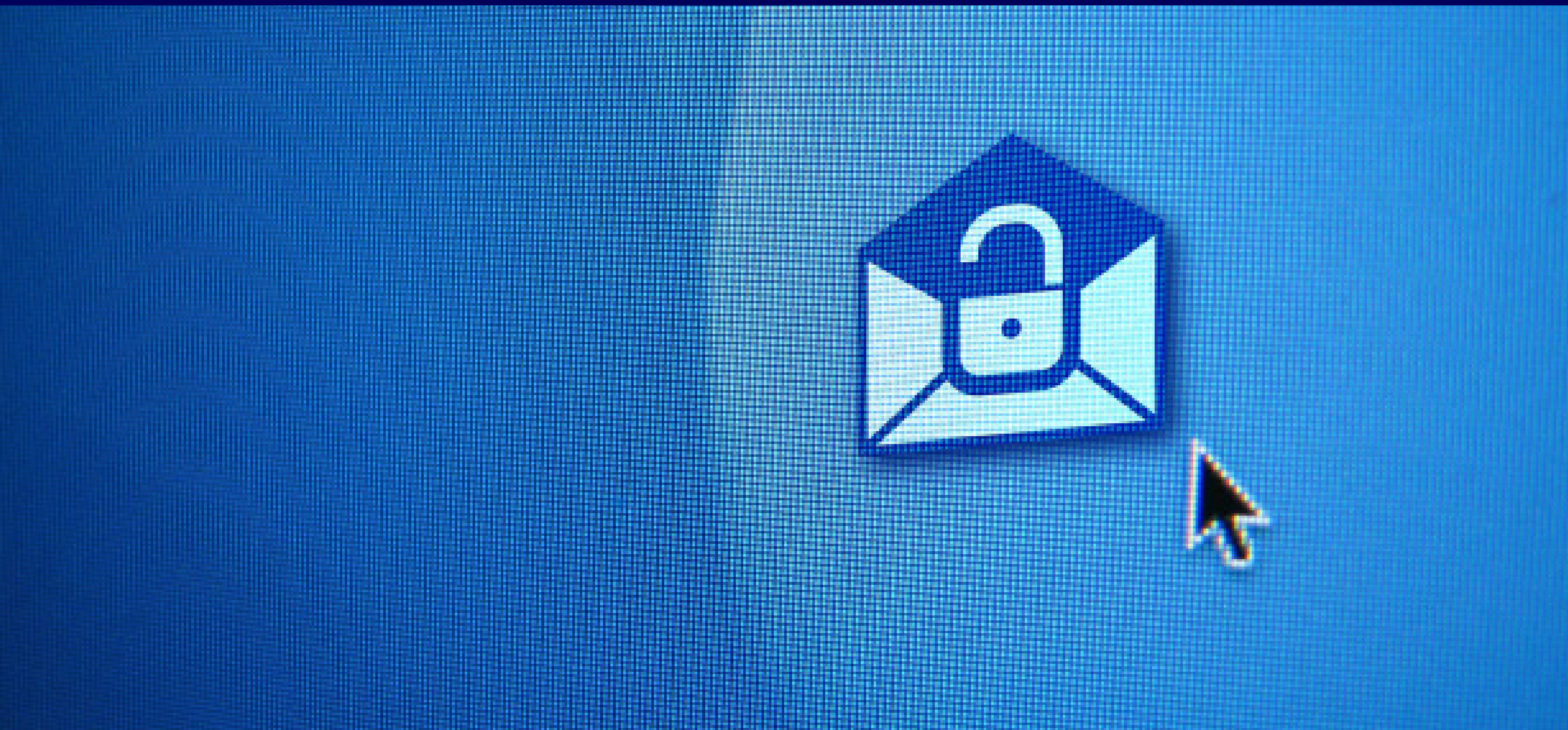
Information on secure e-mail communication

ALDI SOUTH Group



Secure e-mail communication

Introduction

Nowadays, e-mail is a common means of communication. Businesses widely use e-mails to exchange information. The ALDI SOUTH Group also employs this tool to communicate with third parties.

In most cases, the information that is exchanged via e-mail is also confidential, which means that it needs to be protected against manipulation and unauthorised access in particular. Without special protection, data transfer on the Internet between sender and recipient is completely unprotected and can be compared to sending a postcard written with a pencil. Thus, additional security measures are crucial in order to effectively protect e-mail communication.

The ALDI SOUTH Group uses secure standard processes for the exchange of encrypted e-mails to protect confidential information in e-mails.

With this document, the ALDI SOUTH Group would like to provide you with all information necessary to establish a secure communication channel between you and the ALDI SOUTH Group .

Notes for users

The section below explains the relevant terminology connected to e-mail encryption and basic steps for configuring and setting up a secure communication system. The end of this document provides you with brief instructions regarding this topic.

Please contact the appropriate technicians in your company if you have any questions regarding e-mail encryption with the e-mail solution used in your company.

Content

Definition of terms

Encryption

E-mails have to be encrypted to ensure that e-mail communication remains confidential. All information required for encrypting and decrypting e-mails is included in a digital certificate. Both communicating parties must obtain a digital certificate before information can be exchanged in a secure way via encrypted e-mails.

Digital certificates

Digital certificates ensure that only the intended recipient of an e-mail is able to read the information. Such a certificate (also referred to as a user certificate) is issued individually for each e-mail address. The certificate is a digital validation of the sender‘s identity and is used for digitally signing e-mails. In addition, it can be used for encrypting e-mails.

The authentication validates the certified e-mail address for a limited period. Digital certificates are usually valid for a period between one and five years.

Public and private keys

The user certificate consists of two parts: a public and a private key. The private key is used for signing and decrypting e-mails and must never be disclosed. The public key has to be made available to the other party so the e-mail signature can be checked and encrypted e-mails can be sent to the owner of the public key.

Before encrypting the first e-mail, the sender needs to have received the public key as one part of the recipient‘s user certificate. Public keys are usually exchanged by sending a signed e-mail from which the recipient can take the public key. Only then is the sender able to encrypt e-mails using the recipient‘s public key. After receiving the encrypted e-mail, the recipient is able to decrypt it with his private key. Most e-mail programs perform these processes automatically.

Definition of terms

Signatures

In order to automatically check the authenticity of an e-mail address, you will need a digital signature. This enables the recipient to clearly identify the sender. In addition, it guarantees the integrity of the e-mail, since the digital signature is destroyed, much like a seal when a letter is opened, when changing information. Thus, when signing an e-mail, the public key for the certificate is always attached so that the recipient can check the authenticity and integrity of the e-mail.

Signing the e-mail prevents the information contained in the e-mail from being changed, without the recipient noticing. However, they can still be read without any coding . The e-mail has to be additionally encrypted to ensure confidentiality while exchanging information. The most secure way to exchange e-mails is a combination of both signature and encryption.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard process used worldwide for the secure exchange of information via e-mail with certificates. The necessary components for S/MIME are included in most modern e-mail programs; thus, ensuring simple and transparent handling. This means that, provided the user activates the appropriate option in the e-mail program, e-mails are automatically encrypted before being sent and automatically decrypted when being received.

The ALDI SOUTH Group only accepts the S/MIME process for e-mail encryption.

Trust centres

Trust centres are organisations that issue digital user certificates and are responsible for providing and assigning them as well as for ensuring their integrity.

If you have an e-mail system that supports S/MIME, but do not have your own e-mail certificate yet, you may request one from a trust centre. An overview of providers trusted by the ALDI SOUTH Group can be found in the attachment. Issuing a certificate is subject to a charge.

Root certificate

In addition to the user certificate, a root certificate is required for e-mail communication with the ALDI SOUTH Group. The root certificate allows the user to check the authorisation status of the user certificates at the ALDI SOUTH Group, i.e. your system is able to check whether the user certificate has in fact been issued by the ALDI SOUTH Group and whether it is still valid.

Definition of terms

Exchanging certificates

It is necessary to exchange certificates between the communication parties only once before using encryption for the first time. Afterwards, it becomes necessary only if one of the exchanged certificates expires.

Transferring certificates to the ALDI SOUTH Group

Once you have received your personal user certificate from one of the trust centres on the attached list, all you have to do is send a signed e-mail to the communication partner within the ALDI SOUTH Group to make the public key available. You only need to repeat this process if your user certificate has changed, e.g. due to a change of the trust centre.

Receiving certificates from the ALDI SOUTH Group

You will receive the respective user certificate from the appropriate communication party at the ALDI SOUTH Group. The root certificate has to be imported into your terminal (e.g. your PC) once in order to check the user certificates from the ALDI SOUTH Group. The user certificate then has to be assigned to the appropriate contact in the respective e-mail program.

User certificates of the ALDI SOUTH Group are valid for three years.

The root certificate of the ALDI SOUTH Group can be downloaded from the following website: **www.aldi-sued.com/cert**.

Brief instructions for secure e-mail exchange

1 **Import** the ALDI SOUTH Group root certificate.

You can download the root certificate from **www.aldi-sued.com/cert**.

2 **Request** a personal S/MIME certificate from one of the trust centres provided on the list in the attachment and assign it to your e-mail account in the corresponding options of the e-mail software you use.

3 **Send** a signed e-mail to the respective communication party at the ALDI SOUTH Group.

4 **Receive** a signed e-mail from the communication partner at the ALDI SOUTH Group. The signed e-mail contains the user certificate of the communication partner.

5 **Create** a contact for the communication partner at the ALDI SOUTH Group in the corresponding e-mail program and assign the relevant user certificate to the contact.

6 **Select** the encryption option S/MIME when writing an e-mail to the communication partner at the ALDI SOUTH Group.

Attachment

List of supported trust centers

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

Trusted
root certificates: AddTrust External CA Root
UTN-USERFIRST-Client Authentication and Email

Entrust www.entrust.com
Product: Secure E-mail Certificate

Trusted
root certificates: Entrust.net Certificate Authority (2048)

GeoTrust www.globalsign.com
Product: Small & Medium Businesses /
Secure Email Certificates
Enterprise / S/MIME
Trusted
root certificates: GlobalSign Primary Class 1 CA
GlobalSign Primary Class 2 CA

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

Trusted
root certificates: 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