Prefácio

O e-mail é hoje em dia um meio de comunicação utilizado com frequência para troca de informação.

Também a ALDI Portugal mantém o contacto com inúmeros parceiros por e-mail.
As informações que são trocadas por e-mail são na maioria das vezes confidenciais, por isso têm de ser protegidas especialmente contra a manipulação e o acesso por terceiros. Sem uma protecção específica, a troca de dados através de e-mail entre remetente e destinatário é completamente desprotegida, comparável com o envio de um simples postal.
Para uma protecção eficaz da comunicação por e-mail são necessárias medidas de protecção adicionais.
Para a protecção de informações confidenciais contidas nos e-mails, a empresa ALDI Portugal utiliza procedimentos standard para a troca de e-mail codificados.

A empresa ALDI Portugal pretende através deste documento disponibilizar-lhe todas as informações necessárias para criar um sistema de comunicação segura entre si e a ALDI Portugal.

De seguida descreve-se a terminologia relacionada com a codificação de e-mails, bem como os respectivos passos de configuração e instalação.

Apresentamos-lhe também duas variantes de como pode iniciar uma comunicação codificada com a ALDI Portugal. No final deste documento encontra algumas instruções adicionais.

Para questões referentes à codificação de e-mails relacionada com a solução de e-mail utilizada na sua empresa, por favor entre em contacto com o departamento informático da sua empresa.

Codificação

Para preservar a confidencialidade da comunicação por e-mail, os e-mails têm de ser codificados.
As informações necessárias à codificação e descodificação de e-mails, são contidas num chamado "certificado digital" que inclui a chave pública (para todos os parceiros de comunicação) para a codificação e a chave privada (apenas para o proprietário) para a descodificação. Antes de possibilitar a troca segura de informação em forma de e-mail, ambos os intervenientes têm de obter um a chave pública do outro.

Chaves públicas e privadas

O certificado de utilizador é composto por duas partes: uma chave pública e outra privada.
A chave privada é utilizada para a assinatura e a descodificação de e-mails e nunca deve ser pública.
A chave pública deve ser disponibilizada ao parceiro de comunicação, para que possa confirmar a assinatura de um e-mail e enviar e-mails codificados ao detentor da chave pública.

Antes da primeira codificação de e-mails o remetente tem de ter recebido a chave pública, como parte do certificado de utilizador do destinatário. Esta troca efectua-se habitualmente através do envio de um e-mail assinado, do qual o destinatário pode retirar a chave pública. De seguida o remetente poderá codificar o e-mail com a chave pública do destinatário.

Após recepção do e-mail codificado, o destinatário poderá descodificar o mesmo através da chave privada. Este processo é, regra geral, efectuado automaticamente pelos programas de e-mail.

Assinaturas

Para que a fidedignidade do e-mail seja verificada automaticamente, é necessária uma assinatura digital. Através desta o remetente pode ser identificado inequivocamente.
Também é garantida a integridade do e-mail, uma vez que após uma alteração posterior a assinatura digital fica destruída – parecido a um lacre de uma carta quebrado.
Ao colocar a assinatura digital no seu e-mail, é sempre anexada a chave pública, para que o destinatário possa comprovar a veracidade e integridade do e-mail.
Através da assinatura do e-mail evita-se que o seu conteúdo seja alterado, sem que o destinatário o note. Para garantir a confidencialidade do e-mail, este tem de ser adicionalmente

codificado. O procedimento mais seguro para a troca de e-mail é a sua assinatura em conjunto com a codificação.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) é um procedimento standard utilizado mundialmente para a troca segura de informação através de e-mails com certificados. Os componentes necessários para S/MIME estão já integrados na maioria dos programas de e-mail modernos, assim é garantido um manuseamento simples e transparente. Isto significa, que os e-mails, através da activação da opção correspondente, são automaticamente codificados ao enviar e descodificados automaticamente aquando a sua recepção.

A empresa ALDI Portugal apenas aceita o procedimento S/MIME para codificação dos seus e-mails.

Fornecedores de certificados / Trustcenter

Um fornecedor de certificados (também conhecido como Trustcenter) é uma entidade, que emite certificados digitais de utilizadores e é responsável pela sua implantação, concessão e garantia de integridade.
Se tem um e-mail compatível com S/MIME, mas ainda não tem um certificado próprio, pode solicitar o mesmo ao fornecedor de certificados. Em anexo encontra um resumo de fornecedores da confiança da empresa ALDI Portugal.

Certificado raiz

Adicionalmente ao certificado de utilizador é necessário, para a comunicação com a empresa ALDI Portugal, também uma certificado raiz. Com este pode ser controlado o estado de confidencialidade dos certificados da empresa ALDI Portugal. Isto significa, que o sistema utilizado por si, pode controlar se o certificado de utilizador pertence efectivamente à ALDI Portugal e se este ainda se encontra válido.

Troca de certificados

A troca de certificados entre parceiros de comunicação tem de ser efectuada uma vez antes da primeira codificação e será necessária novamente apenas quando um certificado caducar.

Comunicação do certificado à empresa ALDI Portugal:
Se possui um certificado de utilizador pessoal de um dos fornecedores de certificados/Trustcenter da lista anexa e a sua chave pública estiver depositada no Keyserver do fornecedor de certificada/Trustcenter (comp. Instrução cap. 2.1)., o seu parceiro

irá questionar o fornecedor de certificados/Trustcenter e obtém assim automaticamente a sua chave pública.
Se a chave pública não estiver depositada no Keyserver do fornecedor de certificados/Trustcenter, esta poderá ser disponibilizada no portal de certificação ALDI (www.aldi-nord.de/certportal).

Se o certificado de utilizador se tiver alterado, p. ex. por alteração do seu fornecedor de certificados, tem de repetir o procedimento.

Recepção de certificados de empresa ALDI Portugal:
Recebe o seu certificado de utilizador automaticamente com cada e-mail codificado do seu interlocutor da ALDI Portugal.
O certificado de raiz, que também lhe é disponibilizado automaticamente através de um e-mail codificado do seu interlocutor, tem de ser importado uma única vez para o PC do utilizador para efeito de controlo dos certificados do grupo ALDI.
O certificado do utilizador deve ter um contacto associado ao email utilizado. (comp. Instruções cap. 2.5).
Pode-se fazer o download do certificado de raiz da empresa ALDI Portugal através do acesso do Webmessenger, igualmente automaticamente do e-mail do seu interlocutor ALDI a partir do endereço WWW.aldi-nord.de/cert/ , ou recebe-o automaticamente com o e-mail (em anexo) do seu interlocutor ALDI (comp. Instruções cap. 4).

Webmessenger

Com a ajuda de um portal, ou seja, do Webmessenger o parceiro de comunicação recebe um acesso seguro a um e-mail-client. Através do e-mail client disponibilizado pela ALDI o parceiro pode enviar e receber e-mails aos colaboradores da ALDI.

Em seguida, são novamente exemplificados os procedimentos da comunicação com a ALDI Portugal. Para iniciar a comunicação codificada com a ALDI, recomendamos que solicite a opção 1 aquando o pedido do certificado.

1. Opção:

Ainda não tem contacto de e-mail com a ALDI Portugal (também não tem um acesso Webmessenger) e pretende iniciar a comunicação codificada com a ALDI Portugal (troca de chaves através da publicação da chave publica no Keyserver do fornecedor de certificados/Trustcenter).

1	**Beantragen** Sie ein persönliches S/MIME-E-Mail-Zertifikat von einem der Trustcenter aus der Übersicht im Anhang (publizieren Sie Ihren öffentlichen Schlüssel auf dem Keyserver des Trustcenters) (vgl. Anleitung Kap. 2.1 u. 2.2)
2	**Alocação** Envio do certificado pessoal para uma conta de e-mail pessoal através das opções de e-mail-software (comp. Instruções cap. 2.4)
3	**A ALDI Portugal** consulta o Keyserver no anexo Trustcenter e guarda a sua chave pública (dispensa qualquer intervenção)
4	**Recepção** de um e-mail do seu interlocutor ALDI. O e-mail contém o certificado de utilizador do parceiro de comunicação e o certificado de raiz
5	**Introdução** de um contacto para o parceiro de comunicação da ALDI Portugal no programa de e-mail e envio do respectivo certificado de utilizador (comp. Instruções cap. 2.5)
6	**Escolha** da opção de codificação S/MIME na edição de um e-mail para um parceiro de comunicação da ALDI Portugal (comp. Instruções cap. 2.4

2. Opção:

Já recebeu um e-mail de um colaborador ALDI e possui agora um acesso Webmessenger (troca de chave através do Webmessenger).

Unterstützter/s Zertifikatsdiensteanbieter/Trustcenter:

Swiss Sign	https://www.swisssign.com/
Produkt:	Personal ID Silver
Hinweis:	Die Zertifikate sind auch außerhalb der Schweiz gültig.
Vertraute Stammzertifikate sind u.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 Stammzertifikate und Prüfsummen

1. ALDI Nord
   S/MIME Stammzertifikat
   Gültig ab 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 Stammzertifikat
   Gültig bis 06.01.2016

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