格尔安全电子邮件

产品白皮书

上海格尔软件股份有限公司

声明：

Copyright ©2017

上海格尔软件股份有限公司

版权所有，保留一切权利

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

由于产品版本升级或其他原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导。本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

目　录

1 前言 4
1.1 产品背景 4
1.2 名词解释 5
2 产品概述 6
2.1 产品简介 6
3 产品功能及特性 7
3.1 产品基本功能 7
3.2 产品特色功能 9
3.3 产品安全特性 11
4 产品参数 13
5 产品部署 13
6 安装运行环境 15
7 产品界面 15
8 产品证书 17
9 产品支持联系方式 18

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com　　Tel: 021-62327010　　Fax: 021-62327015

1 前言

1.1 产品背景

随着计算机技术和通信技术的飞速发展，信息化的浪潮席卷全球。其中，作为当前和未来网络上重要沟通方式之一的电子邮件，也将起着越来越重要的作用。电子邮件的使用不可避免会涉及众多敏感数据，如财务报表、法律文件、电子订单、设计方案等。然而，由于互联网的开放性、广泛性和匿名性，通过传统电子邮件传输信息存在很多安全隐患：

- 用户名和口令的弱点

  传统的邮件系统以用户名和口令的方式进行身份认证。用户名和口令方式本身的不安全因素（口令弱、明文传输容易被窃听等）会导致整个邮件系统的安全性下降。

- 信息的机密性

  邮件内容往往包含很多商业或政府机密，因此必须保证邮件内容的机密性。然而，传统的邮件系统中，邮件以明文的方式在网络上流通，很容易被不怀好意的人非法窃听，造成意料之外的损失；而传统邮件系统中的邮件本身也是以明文的方式存放在邮件服务器中的，系统管理员或非法得到服务器权限的人可以查看所有的邮件，没有任何对邮件机密性的保护。

- 信息的完整性

  传统的邮件发送模式中，邮件中的敏感信息和重要数据很容易在传输过程中被恶意篡改，使得邮件接收者不能收到完整的邮件，造成不必要的损失。

- 信息的不可抵赖性

  由于传统的邮件工作模式（用户名＋口令、明文传输等）对邮件没有任何的保护措施，邮件发送和接收的双方都不能肯定邮件的真实性和完整性，同时双方都可以否认对邮件的发送和接收，很难在出现事故的时候追查某一方的责任。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

1.2 名词解释

名词	解释
PKI	Public Key Infrastructure 即公钥基础设施，是利用公钥理论和技术建立的提供信息安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。
CA	Certificate Authority，数字证书中心，作为权威的第三方负责发放数字证书。
数字证书	Certificate，数字证书中心签发的用于代表实体身份的一段电文。
LDAP	(Light Weight Directory Access Protocol) 是一种轻量级的目录存取协定，帮助客户从各个角落连接到目录服务器中。
邮箱用户	是指使用格尔安全电子邮件的归属者。
加密/解密	使用计算机密码技术，对数字信息进行转换保护，形成新的信息，称为加密；将加密的信息还原成原文信息，称为解密。
数字签名	采用 PKI 技术，先对原文信息进行摘要，然后通过私钥进行签名，生成签名信息（只能通过私钥进行签名，且签名过程不可逆），以保证原文数据的完整性和不可否认性。
机密性	邮件加密有助于保护电子邮件的内容。 只有预期收件人才能查看内容，邮件内容一直得到保密，可能收到或查看邮件的任何其他人都无法知道此邮件。 在邮件传输和存储过程中，加密可帮助提供机密性。
不可否认性	是指对行为的确认，确定行为必须是某人或某机构所为，不能否认，数字签名通过非对称密码技术和 PKI 管理体制，保证不可否认性的实现
数据完整性	表示数据没有遭受以非授权方式所作的篡改或破坏。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

2 产品概述

2.1 产品简介

格尔安全电子邮件系统（以下简称 KMAIL）是格尔公司自主研发的基于 PKI 技术的、易于实施的、完善的、WEB 方式访问的网络安全应用产品。产品部署在网络中，向用户提供基于 PKI 技术的安全电子邮件服务。系统不仅能够确保收发邮件的**机密性**、**完整性**和**不可抵赖性**，还可以保证邮件的**存储安全性**。

系统以软件方式发布，由用户自行安装在提前准备好的服务器上，系统软件、邮箱账户、邮件数据等都存放在该服务器上。其中邮件数据、备份文件可以配置存储到专门的存储服务器。邮件系统的服务器必须和 SSL 安全网关结合使用，因为用户和管理员必须经 SSL 安全认证网关强身份认证后方可访问邮件系统。另外收发加密邮件还需要配置证书服务器（一般来说是 CA 系统将证书发布在 LDAP 服务器上的），用来查询邮箱用户对应的加密证书。

系统保证收发邮件及存储邮件的安全性，基本原理如下：

- 发件人使用邮件接收者的数字证书（加密证书公钥）对电子邮件的内容和附件进行加密，加密邮件只能由接收者所持有的加密证书的私钥才能解密，从而确保只有邮件接收者才能阅读，确保电子邮件在传输的过程中不被他人阅读、截取和篡改；

- 邮件使用发件人的数字证书（签名证书私钥）对电子邮件进行数字签名，邮件接收者通过验证邮件的数字签名来验证邮件是否被篡改，并判断发件人的真实身份，确保电子邮件的真实性和完整性，并防止发件人抵赖。

- 邮件服务器里的邮件也是使用证书加密的，极端情况下，即使邮件服务器内容全部被人拿走，别人也无法看到有意义的邮件内容。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

3 产品功能及特性

3.1 产品基本功能

- 邮件收发

以浏览器/服务器模式(B/S)方式提供可视化的邮件编辑、附件选择、邮件发送、邮件接收功能，对于邮件接收人可包括明送、抄送、暗送三种类型。

- 邮件群发

支持将同一封邮件发给多个收件人。

- 邮件转发

支持邮件转发功能，包括附件转发。

- 邮件回复

对于接收到的邮件，收件人可使用邮件回复功能自动创建邮件收件人、邮件标题和正文内容,并呈现编辑状态。邮件回复功能包括单人回复和全部回复两种。

- 邮件草稿

对于编辑状态的邮件，可以手动将其保存为邮件草稿，可在草稿箱中找到并再次编辑该邮件。

- 再次编辑

对于已发送的邮件，发件人可以在发件箱中查询到，并再次编辑发送。

- 自动回执

可设置邮件要求回执功能，以了解收件人是否已经收到邮件。

- 邮件状态标记

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

所有接收到的邮件都包括已读和未读两种状态，并可以手动设置。

- 邮件退信

对于已经发送的邮件，如果没有正确到达，系统会给发件人退信，并说明未到达原因。

- 邮件导出

用户可以导出邮件，以便在离线环境下查看邮件（邮件格式是标准格式，一般客户端工具都能查看）。

- 邮件夹管理

提供收件箱、已发送、草稿箱、已删除等默认邮件夹，也可以自定义邮件夹。

- 邮件删除

提供两级删除功能，邮件删除时先保存到已删除邮件夹，在用户清空已删除邮件夹时才真正删除。

- HTML 邮件

支持发送和接收 HTML 标准格式的邮件。

- 邮件统计

提供邮件统计功能，用户可以查看指定邮件夹的邮件数与未读邮件数，同时可查看所有邮件夹合计邮件数和未读数以及邮箱容量的总体情况。

- 邮件查询

可全局查询邮件，也可根据邮件的主题、发件人、收件人、邮件夹、时间等进行条件查询。

- 备份恢复

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

系统提供对系统数据、邮件数据的自动备份，该自动备份进程在后台独立运行，可以通过配置指定其备份动作的运行时间，避免与使用高峰冲突。支持备份在本服务器或外置存储服务器。

3.2 产品特色功能

- 支持标准邮件格式

邮件格式采用标准的 MIME、S/MIME（加密邮件）格式，方便跟其它邮件系统或邮件客户端兼容。

- 支持客户端工具收发邮件

支持常用客户端工具（foxmail、outlook）收发普通邮件，并支持常用客户端工具打开加密邮件。

- 一用户多邮箱机制

一个用户可设置多个邮箱，也就是使用一张用户证书登录可管理多个邮箱。

- 重要邮件标记

发件人可在编辑邮件时设定邮件标记，比如重要标记。接收人在收件箱中看到此邮件时，可以通过标记知道邮件的重要性。

- 收件人输入联想机制

写邮件输入收件人地址时，提供自动联想功能，可根据中文、英文、拼音首字母自动列出符合条件的收件人。并且支持用户已经发送过的邮件地址自动加入联想库功能。

- 定时发送

用户可以指定邮件在未来的指定日期和时间自动发送。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

- 新邮件提醒

当用户登录系统进行操作过程中接收到新邮件，系统将以更换浏览器页面标题并闪烁的方式提醒用户有新邮件到达。

- 邮件撤回

在邮件发送完成但接收者还未阅读时，发件人可在发件箱内查询得到该邮件并执行邮件撤回功能。

- 邮件回复转发标记

回复或转发过的邮件在邮件列表中将有明显标记。

- 自动保存草稿功能

当用户在编辑邮件时，系统将定时自动保存草稿。

- 组邮箱功能

组邮箱可以理解为一个转发邮箱，组邮箱可绑定多个用户邮箱，也可随时更换绑定的用户，用户不可登录组邮箱，但发给组邮箱的邮件会转发给绑定的用户邮箱。

- 公共邮箱功能

公共邮箱可理解为一个职位邮箱，可绑定多个用户，也可随时更换绑定的用户，所有绑定的用户可以共同登录此邮箱查看邮件，适合给人员变动较大的职位创建公共邮箱。

- 邮件收发权限控制

可灵活配置发送本域邮箱或外域邮箱的权限。

- 自动删除邮件功能

用户可根据时间设置自动删除在“已删除”邮件夹中的邮件。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

- 丰富的联系人选择机制

系统通讯录有常用联系人、个人组、个人通讯录、公共组、公共通讯录等多种分类，用户可提供树状组织结构、智能输入联想、列表过滤查询等多种方式选择联系人。

- 多种账户注册功能

系统支持手工录入、导入文件、自主注册等多种方式进行账户的注册，方便管理员的工作。

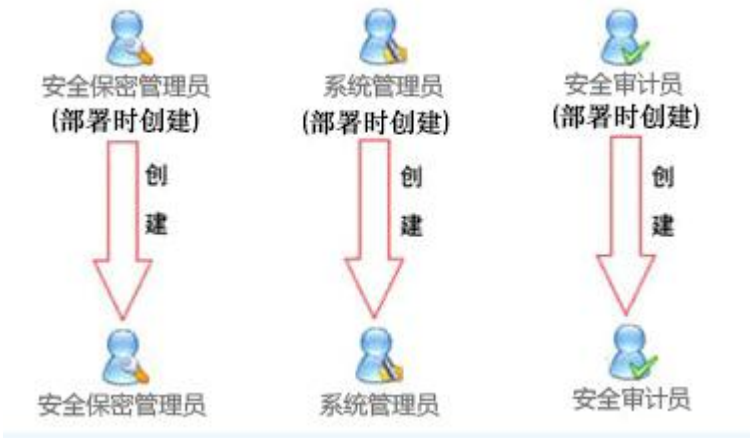
- 网盘功能

系统自带网盘功能，结合网盘文件，邮件发送理论上可支持无限大附件。

3.3 产品安全特性

- 三权分立安全管理

系统提供系统管理员、安全保密管理员、安全审计员三种管理员分权管理模式进行系统的管理。



- 基于 PKI 的强身份认证

系统是 B/S 架构的 WEB 应用系统，用户和管理员都是通过基于 PKI 证书管理体系的安全认证网关访问 WEB 管理页面的，安全认证网关提供双向认证机制，

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

客户端在访问系统时需要提供合法的用户证书，客户端在提交数据到服务端时，将建立一条加密的安全通道，防止提交的数据被第三方截取，与此同时，邮件系统对用户全程操作环节进行日志记录。

- 系统访问的安全

系统是 B/S 架构的 WEB 应用系统，用户和管理员都是通过安全认证网关访问 WEB 管理页面的，安全认证网关提供双向认证机制，客户端在访问系统时需要提供合法的用户证书，客户端在提交数据到服务端时，将建立一条加密的安全通道，防止提交的数据被第三方截取。

- 邮件内容安全

系统提供发送加密邮件的功能，加密数据是一个符合 PKCS#7 标准的签名加密数据（使用发件人签名证书私钥签名和使用收件人加密证书公钥加密），没有对应收件人的加密证书私钥，其它人是解不开邮件的，另外，收件人还可以通过验证签名来判断数据的完整性及发送者的真实性。

- 密级控制

系统提供密级定义功能，可定义系统密级、用户密级、邮件密级、附件密级。通过各种密级关系比较，控制邮件的安全流转。

- 邮件流向控制

主要用来控制邮件的流向，定义了

  - 跨域发送邮件的流向控制
  - 跨部门发送邮件的流向控制
  - 不同用户级别间发送邮件的流向控制
  - 不同用户密级间发送邮件的流向控制

流向控制的具体措施有：禁止发送、审批后发送、免审批发送

审批机制可以是：单人审批、多个审批、多级审批

审批人的选择可以根据策略定义，可以是：指定单个或多个部门领导审批，

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

指定单个或多个用户级别审批，指定单个或多个人员审批等

- 邮件存储安全

存储在系统中的邮件都是加密过的邮件，没有对应的证书，即使获取到邮件，也无法看到邮件内容。管理员也无法看到邮件内容。

- 应用安全

系统对常见的 WEB 系统攻击手段（如 XSS 攻击、SQL 注入攻击）进行了防护，保障系统的安全。

4 产品参数

邮箱用户数支持：1 万（由服务器性能和用户使用率决定）

邮件附件大小限制：180M

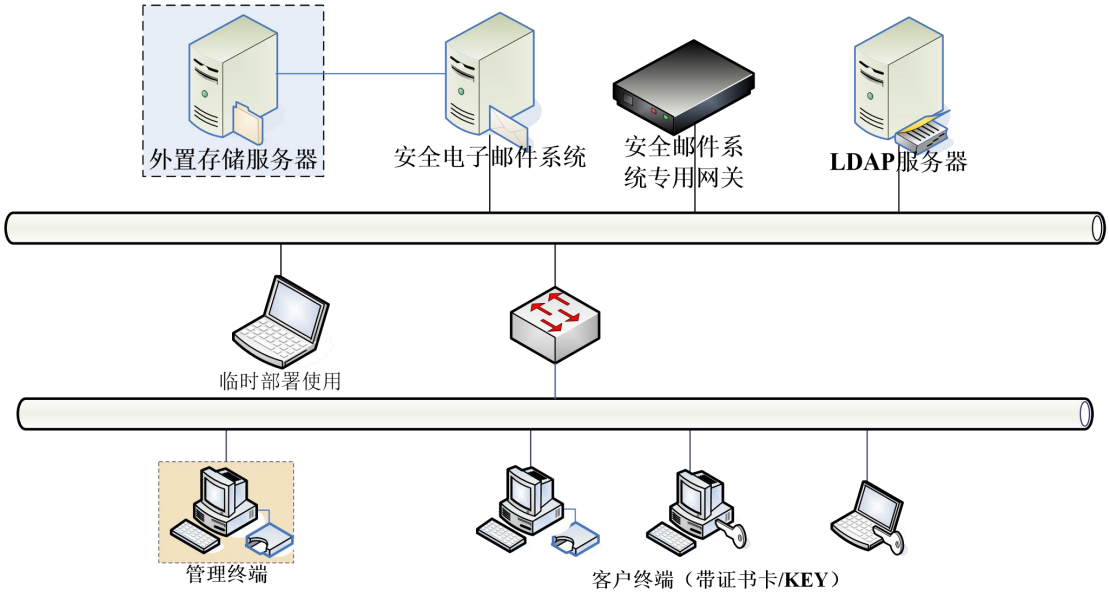
网盘附件大小限制：单个网盘附件最大 2G，总大小无限制

邮件正文最大：约 50 万个字

5 产品部署

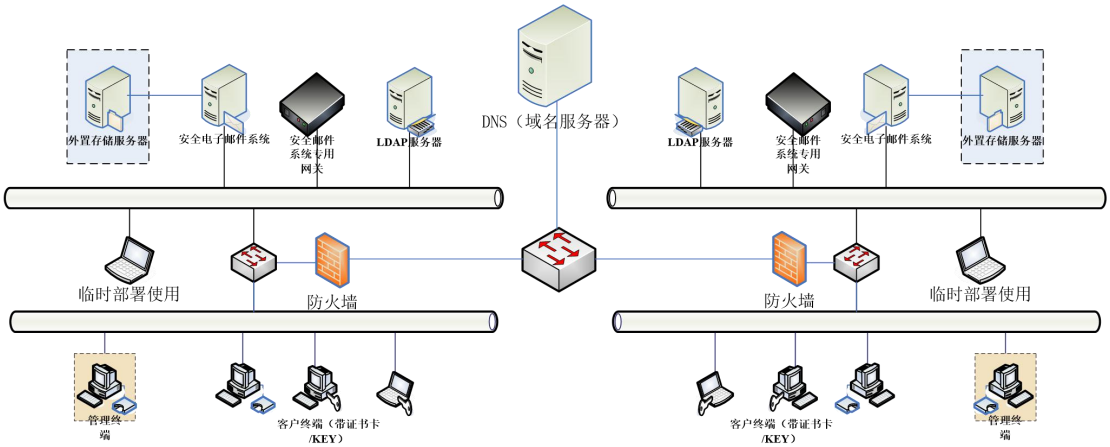
单系统部署：

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015



图表 1 网络拓扑图一

多系统互联部署：



图表 2 网络拓扑图二

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

6 安装运行环境

服务端配置：

P4 3G 双核以上、 2G 内存以上、500G 存储以上

操作系统：Red Hat Enterprise Linux 5、6 64 位

客户端配置：

P4 2G 以上、1G 内存以上

操作系统：windows xp、windows7，支持 32 和 64 位系统

浏览器推荐使用 IE，推荐版本 6、7、8、9、10，非 IE 浏览器支持 chrome、FireFox、safari。

7 产品界面

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

8 产品证书

《公安部销售许可证》

《保密局产品检测证书》

《商密产品证书》

《软件著作权登记证书》

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号中铁中环时代广场 4 号楼 6 楼
URL:http://www.koal.com Tel: 021-62327010 Fax: 021-62327015

9 产品支持联系方式

上海格尔软件股份有限公司

电话：021-62327010

传真：021-62327015

地址：上海市江场西路 299 弄 5 号中铁时代广场 4 楼 6 楼（近万荣路）

邮编：200436