格尔网络保险箱(NSS)

产 品 白 皮 书

上海格尔软件股份有限公司

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

版权声明:

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

目　录

1　背景 4
1.1　名词解释 4
2　产品概述 5
3　产品主要功能 6
4　产品特色 7
4.1　网络保险箱系统实现了安全的存储 7
4.2　安全并且灵活的授权方式 7
4.3　本地使用，远端存储 8
5　产品部署 8
6　产品参数 9
7　客户端运行环境 9

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

1 背景

随着信息化程度的日益提高，信息技术被广泛的应用于各个领域。数据，特别是那些包含了组织内部核心机密信息的文档，成为了不断增长的重要资源和财富。如何安全的存储、共享成为组织面临的重要问题。然而，目前的现状是:

- 涉密的文档被分散存储在组织内部的 PC 或服务器上。无法统一的管理。
- 文档即使被集中存储，对文档的保护也只是采用了操作系统所提供的权限控制机制。
- 文档如果被加密存储，则不便于在多人之间共享。

针对以上问题，格尔软件推出了网络保险箱。

1.1 名词解释

- NAS: Network Attached Storage，网络连接存储。是一种专业的网络文件存储及文件备份设备。NAS 是基于 LAN 的，按照 TCP/IP 协议进行通信，面向消息传递，以文件的 I/O 方式进行数据传输。
- 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。本文中涉及代表用户身份的用户证书和代表服务端身份的站点证书（服务器证书）。
- LDAP: (Light Weight Directory Access Protocol) 是一种轻量级的目录存取协定，提供客户从各个角落连接到目录服务器中。本文中专指用于 CA 发布证书及黑名单的服务。

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

- 黑名单：通常所说的 CRL（Certificate Revoke List ），因时间或者安全原因被废除的证书列表，一般发布在 LDAP 上。
- 数字信封：数字信封技术是 PKI 技术的重要应用，广泛用于数据保护，数据加密技术。它采用非对称加密算法和对称加密算法相结合来保护数据安全，兼顾了安全性和效率。

2 产品概述

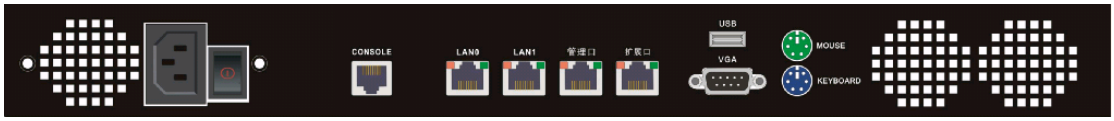
网络保险箱是一套数据网络集中安全存储系统，里面有三种类型的文件，私人文件，部门公共文件和他人授权文件。私人文件是管理员在服务器上为个人开辟一块私有空间，对存放其中的文件进行加密保护，谁都不能看到私人文件中的内容，除了用户自己。部门公共文件是整个部门共享，除了这个部门的人和被授权的人，其他人也不能看到其内容。系统使存储的资料能够安全的集中管理，进行统一有效的备份，达到资料更为安全的存储。他人授权文件提供了一种文件授权的机制，让用户和用户之间能够安全的交换信息，达到信息共享的目的。

网络保险箱由客户端软件和服务器端硬件组成。结合用户已有的文件服务器或 NAS 设备即可组成完整的安全存储系统。

客户端完成文件加密，解密等运算。服务器负责控制，调度。客户端和服务器通讯的网络中，文件也是加密传输，加密存放。客户端界面采用 Explorer 风格，美观，简单，易用并支持拖曳操作。普通用户不用任何培训能够轻松使用。

图表 1 网络保险箱服务器前面板

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com



图表 2 网络保险箱服务器后面板

（以上产品外观图仅做参考，具体外观及接口以实物为准）

3 产品主要功能

功能	说明
基于数字证书的用户认证	用户的认证完全基于 PKI 体系
高强度的文件加密	存储在网络保险箱中的文件是经过加密的，即使是系统的管理员未经文件所有者的授权也无法查看其中的内容
文件加密传输	从用户客户端到存储系统之间的信息传输都是加密的
文件服务器空间配额控制	可设置每个用户所能使用的文件服务器的存储空间。使文件服务器被合理的分配
灵活的共享机制	用户可通过授权的方式将文件共享给他人使用。并且授权时可以控制是被授权用户是否可修改
方便且安全的公共文件夹	为每个注册的部门提一个公共文件夹，方便部门内用户安全的交换信息

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

支持 MS Office	加入到网络保险箱中的 Office 文档（word 档及电子表格等），可以从保险箱中直接打开，并修改。保存后直接存入网络保险箱
支持多种存储服务器	网络保险箱可以使用 Windows 及 Linux 文件服务器及 NAS 作为文件服务器
共享文件的访问记录	文件的所有者可以查看存储在网络保险箱中并授权给他人使用的文件的最近的使用记录

4 产品特色

4.1 网络保险箱系统实现了安全的存储

以往的存储系统只强调的存储数据的安全。而网络保险箱从内容安全上进行加固:

1. 存储在网络安全存储系统中的内容是加密的，即使是系统的管理员在未经授权的情况下也无法查看其中的内容。
2. 用户只能看到和打开自己存储的文件或者别人授权给自己的文件。
3. 用户到网络安全存储系统之间的信息传输都是加密的。
4. 非常安全地授权给他人，而不用担心未授权用户能够看到它。

4.2 安全并且灵活的授权方式

网络保险箱提供了基于数字信封技术的授权方式。

数字信封中采用了单钥密码体制和公钥密码体制。文件的授权者首先利用随机产生的对称密码加密文件，再利用被授权者的公钥加密对称密码，被公钥加密后的对称密码被称之为数字信封。被授权者在打开文件时，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密文件。

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

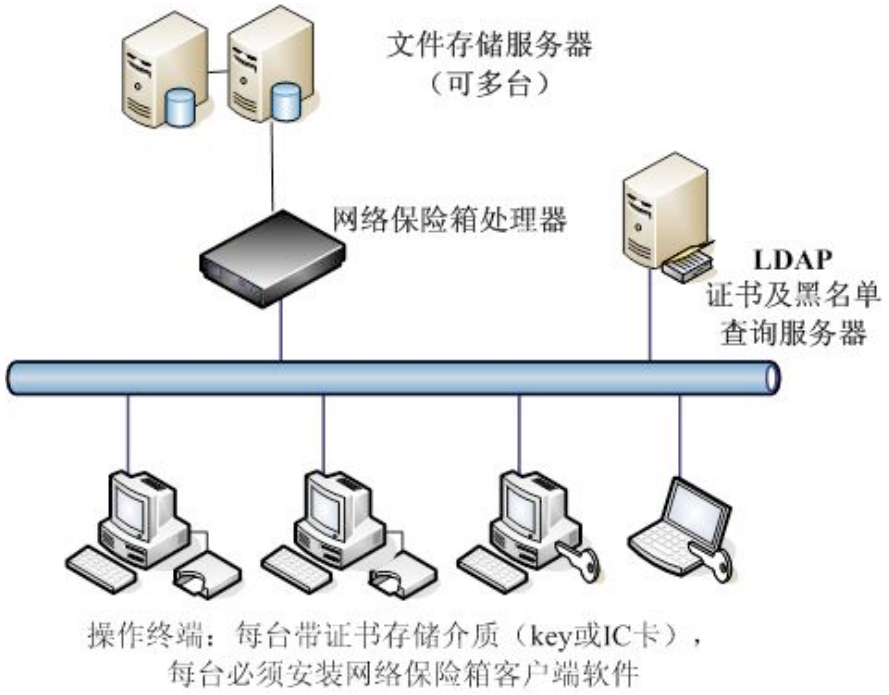
用户利用系统提供的授权机制，可以灵活的将文件授权给系统内注册的任意用户。

4.3 本地使用，远端存储

文件被加入到网络保险箱后，被安全的存储在文件服务器上。当用户想要使用文件时，只需从本地登录到保险箱。然后就可以像使用本地存储的文件一样使用存放在网络保险箱中的文件。而并不需要关心文件的加解密及上传下载的问题。网络保险箱都会自动完成。

5 产品部署

网络保险箱服务器与文件服务器采用的是并联方式部署。网络保险箱服务器和文件服务器物理连接是在同一网络中。用户必须同时能够访问网络保险箱服务器和文件服务器。



图表 3 网络保险箱系统拓扑图

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

6 产品参数

格尔网络保险箱服务端采用专用硬件，产品具有多个型号:

	E-2010	E-2020	G-4020
设备高度	1u	1u	2u
网络接口	4*100M	4*100M	4*100M/1000M
电源指标 数量: 电压（V）: 电流（A）: 功率（W）:	 1 90~264 2~4 180	 1 100~240 5~8 200	 1 90~264 2~4 250
工作温度	0°C--40 °C	0°C--40 °C	0°C--40 °C
工作湿度	5%--95% RH，不凝结	5%--95% RH，不凝结	5%--95% RH，不凝结
最大用户数	50	200	1000

注：上述所有规格及参数若有变动恕不另行通知，请以厂家提供的最终配置为准。

7 客户端运行环境

使用网络保险箱客户端软件的机器推荐配置如下:

CPU: P4 1.0G 以上

内存: 256M 以上

操作系统: Win2000 + SP4 以上

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
Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com