

格尔 USB 守护神(USN) 产 品 白 皮 书

上海格尔软件股份有限公司

版权声明：

本文件中出现的全部内容，除另有特别注明，版权均属上海格尔软件股份有限公司（以下简称格尔软件）所有，未经格尔软件书面许可，任何人不得以任何形式擅自拷贝、传播、复制、泄露本文件的全部或部分内容。

目 录

1	概述.....	4
1.1	背景.....	4
1.2	名词解释.....	4
2	产品概述.....	6
2.1	产品简介.....	6
2.2	产品组成.....	6
3	产品主要功能特点.....	7
4	产品特色.....	8
5	产品部署.....	9
5.1	行业级部署.....	9
5.2	企业级部署.....	10
6	产品参数.....	11
7	客户端运行环境.....	12

1 概述

1.1 背景

随着 USB 技术的成熟和应用的普及 (每台计算机都具备了 USB 接口), 基于 USB 技术的设备层出不穷 , 如 USB 硬盘、USB 鼠标、USB 打印机等等。USB 存储设备以其容量大 , 速度快 , 携带方便 , 使用简单 (windows 自带驱动 , 无须安装) 等特点受到广泛青睐。

但是 , USB 存储设备带来方便性的同时 , 也对信息的安全性带来隐患。首先 , 系统外部人员或者系统内部人员可以轻易地使用 USB 设备将内部信息带出而不留任何痕迹 ; 其次 , USB 存储设备种类繁多 , 包括 U 盘、USB 硬盘、MP3、数码相机等都具有 USB 的存储功能 , 都可以接入系统带走信息 , 可谓防不胜防。

因此 , 如何实现对 USB 存储设备进行有效控制 , 防止信息通过 USB 存储设备外泄是众多部门亟待解决的问题。

1.2 名词解释

术语	解释
USB	Universal Serial Bus 通用串行总线

USB 存储设备	通过 USB 接口存储数据的设备 ,包括 U 盘、USB 硬盘、MP3、数码相机、硬盘盒等等 , 不包括通过专用软件进行读写的 USB 存储设备 , 也不包括非 USB 接口的移动存储设备 ,例如 SD 卡、CF 卡、MMC 卡等。
USN	USB Security Numen (USB 安全守护神)
注册中心	注册并格式化 USB 存储设备的系统
控制中心	进行 USB 存储设备接入认证的系统
USN 客户端	安装在计算机上 , 用于控制 USB 存储设备接入
内部 USB 存储设备	在注册中心注册的 , 已授权的合法 USB 存储设备
外部 USB 存储设备	未注册的 USB 存储设备
内部计算机	已安装 USN 客户端的计算机
外部计算机	未安装 USN 客户端的计算机
证书方式	USB 存储设备加载时采用证书认证的方式
口令方式	USB 存储设备加载时采用口令认证的方式

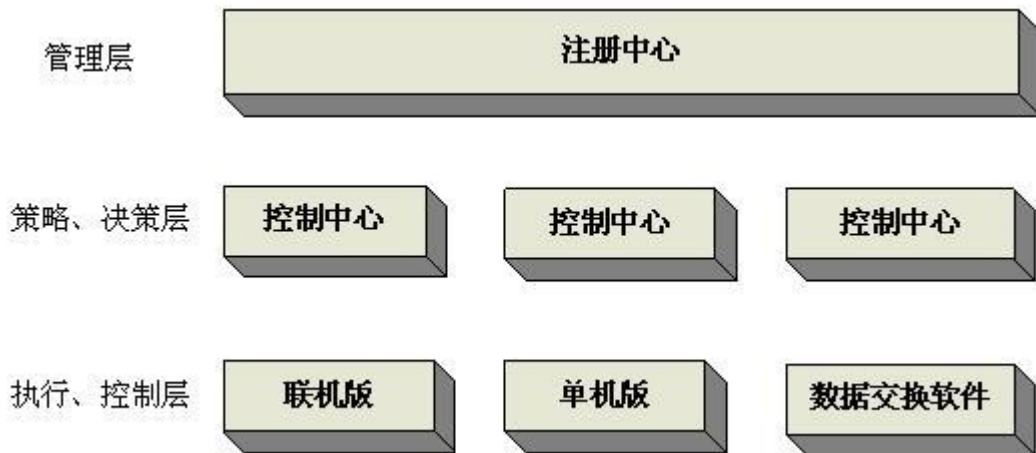
2 产品概述

2.1 产品简介

格尔 USB 守护神是一款对 USB 存储设备进行完善、严格管理控制的产品。产品将系统分为内部计算机与外部计算机，将 USB 存储设备分为内部 USB 存储设备与外部 USB 存储设备，实现外部计算机无法识别内部 USB 存储设备，内部计算机拒绝外部 USB 存储设备接入，同时对内部 USB 存储设备的接入和使用也根据策略进行细致、有效的控制，可以有效防止内部信息通过 USB 存储设备泄密。

2.2 产品组成

本产品分为客户端和服务端，服务端包括注册中心、控制中心，形态为专用硬件，提供 WEB 操作界面；客户端包括联机版、单机版和交换软件，形态为软件方式。产品的逻辑组成如下：



图表 1逻辑结构

- 注册中心：USB 存储设备的统一管理中心，负责对 USB 存储设备注册操作，将 USB 存储设备标记为注册中心管辖范围内的合法设备。
- 控制中心：USB 存储设备的认证策略和决策中心，一方面提供 WEB 界面设置管辖范围内的 USB 设备接入的策略，另一方面提供认证决策服务，根据策略为客户端认证请求进行决策。每个独立的网络环境或者独立的职能范围都应部署一个控制中心。
- 客户端控制软件：安装在客户机上，对 USB 设备进行监控，根据控制中心的策略对 USB 设备进行相应的控制，记录设备的接入记录。客户端控制软件分为联机版和单机版，联机版软件必须根据控制中心的策略控制 USB 存储设备的接入，单机版软件根据本地策略控制 USB 存储设备的接入。另外，数据交换软件用于在外部 USB 存储设备和内部系统之间交换数据。

3 产品主要功能特点

1. USB 存储设备的独特标记功能，能够对 USB 存储设备进行唯一性标记，确保 USB 存储设备无法仿冒。
2. 统一注册功能，可以对 USB 存储设备发放、使用分布进行统一的管理。
3. 未注册的 USB 存储设备无法在内部系统使用，注册过的 USB 存储设备在外部系统无法使用。
4. 管理员通过 Web 方式远程管理，非常方便。

5. 系统自动识别并控制 USB 存储设备，不影响其他 USB 设备（如 USB 鼠标、USB 键盘等）的正常使用。
6. 任意联机客户端的 USB 存储设备的接入策略都可以通过服务端进行统一配置管理。
7. 系统对 USB 存储设备接入的策略可以分为只读、完全控制和禁用。
8. 服务端可以实时获取并记录 USB 存储设备的接入日志。
9. 内置数据库，也可以支持外接数据库。
10. 系统一经安装，会在后台自动启动，无法恶意删除、终止、卸载或破坏。
11. 系统不占用系统资源，不影响 Windows 系统运行效率。
12. 系统实现内部 USB 设备数据写入自动加密，读取自动解密。
13. 系统能够对各种 USB 存储设备进行控制，如 U 盘、MP3、数码相机、USB 软盘、USB 刻录机等，
14. 系统支持大容量 USB 存储设备，如 USB 硬盘等。
15. USB 存储设备的认证支持口令方式和证书方式。
16. 数据交换功能，能够安全可靠的与外部 USB 存储设备进行数据交换，对交换的数据进行详细记录。
17. 系统支持单机环境的 USB 存储设备控制。
18. 客户端与服务端之间采用加密通讯，保证安全性。

4 产品特色

- 安全、完善的系统。安全的一个显著特征是系统的建设者不是系统安全的最大威胁者，即建设者无法破解系统。主要体现在以下两个方面：
 - 系统的建设者无法自己制作一个 USB 存储设备可以在系统内部正常使用。
 - 系统建设者无法自行解密系统内部的 USB 存储设备。
- 采用驱动技术，实现磁盘级的透明加解密，使用简单，安全可靠。
- USB 存储设备的控制策略详细、丰富，可以对内部 USB 存储设备进行有效的管理，可以完全避免 USB 存储设备丢失（其他人获取后到内部系统使用）造成的安全隐患，同时也可以杜绝 USB 存储设备在内部系统内的随意使用。
- 统一管理，分散应用，对于不同规模、不同需求的环境都有相应的解决方案。
- 实时、完整的日志审计。对注册、认证和交换操作都有详细的审计。

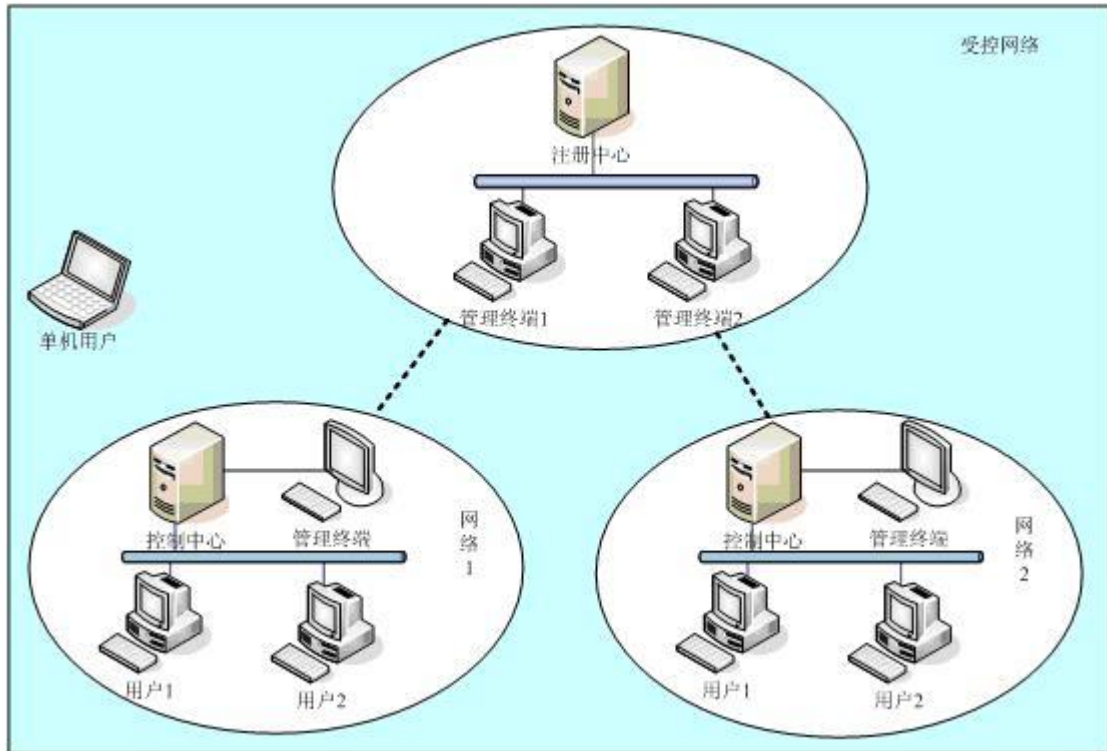
5 产品部署

5.1 行业级部署

应用环境：

- 行业内部或者大型企业，人员、网络规模庞大，具有统一的管理部门。
- 各个职能部门相对独立、网络隔离或者处于不同地域。

针对以上环境可以采用注册中心与控制中心独立部署，即在总部建立注册中心，负责整个系统范围内的 USB 存储设备的注册、发放、管理，在各个独立网络内或者独立的职能部门内部署控制中心，独立控制本范围内的 USB 存储设备接入，如下图：



图表 2 行业级部署

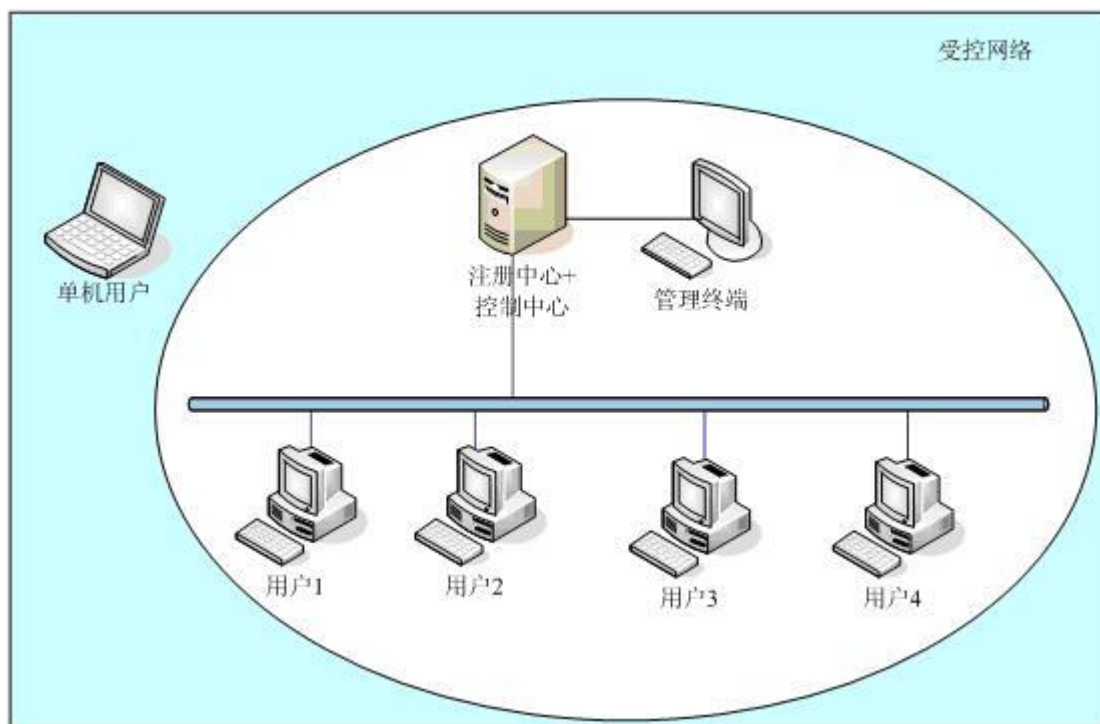
5.2 企业级部署

应用环境：

- 独立的职能部门或者中小企业。
- 网络连通、规模较小。

针对以上环境可以采用注册中心与控制中心联合部署，即注册中心与控制中

心合为一体，由统一的管理员进行 USB 存储设备的注册、发放、管理，以及控制本范围内的 USB 存储设备接入，如下图：



图表 3 企业级部署

6 产品参数

格尔 USB 守护神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 :	1	1	1
电压 (V):	90~264	100~240	90~264
电流 (A):	2~4	5~8	2~4
功率 (W):	180	200	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	100	200	5000

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

格尔 USB 守护神客户端推荐配置如下：

CPU：P3 800M 以上

内存：256M 以上

操作系统：win2000，winxp，win2003