安全存储服务系统

二 OO 六年十二月

安全存储服务系统提供加密的文件存储服务，满足个人的文件安全存储，同时提供工作组内的加密文件共享服务，为个人或工作组提供安全的文件存储环境。

1 系统结构

安全存储服务系统是集中存储的文件服务器，提供文件透明加密存储和加密共享功能，并实现文件访问的传输加密。安全存储服务系统从软件结构上包括安全存储服务器和安全存储客户端。安全存储服务器由安全操作系统、加密文件系统构成，并提供 samba 服务；客户端用户通过 smb 协议访问文件服务，把服务器的文件目录映射到本地目录，就像访问本地文件一样访问远程文件；客户端访问安全存储服务器时，必须经过基于智能卡的身份认证，并且所有客户端与安全存储服务器的交互数据加密传输。

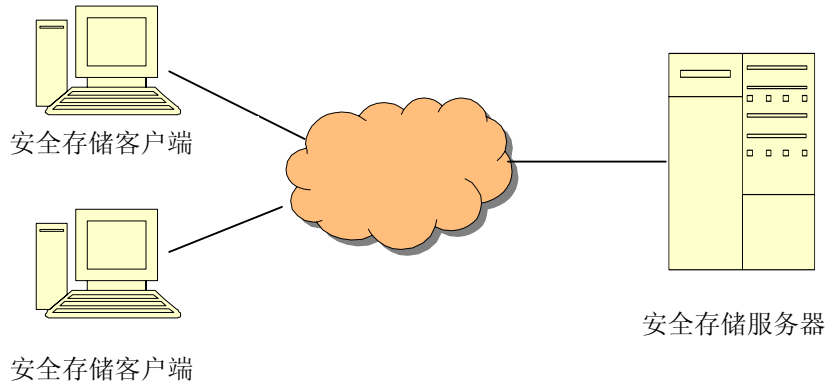

图 1 安全存储服务系统

2 系统功能

安全存储服务系统的主要功能是为政府部门、企事业单位内部提供方便、安全的文件存储环境。系统功能具体包括:

- 提供保险箱方式的个人数据加密；
- 提供工作组范围内加密数据的共享；
- 提供网络邻居方式访问个人保险箱；
- 提供 VPN 虚拟专网实现客户端与服务器之间的数据加密；
- 用户使用 usb key 的密钥作为解密个人保险箱数据的发起密钥；

3 用户使用手册

3.1 初始化客户端

由于安全存储服务系统客户端具有虚拟专网的功能，第一次启动安全存储服务系统客户端（Milstar 客户端）时，虚拟专网系统会进行初始化，并提示安装虚拟网卡。初始化完成后，Milstar 主界面上便会给出信息提示。如图 2 所示。

图 2 客户端主界面

3.2 安全通道配置

安全通道配置是配置虚拟专网的安全隧道。点击主界面的配置菜单，进入配置界面如图 3 所示。

（1）服务器地址和端口。

（2）通信协议。

（3）认证方式配置。可以采用下列三种配置方式：

- 用户名+密码。这种方式不相对安全性较低。
- 证书+密钥：需要选择分发给用户的 ca、cert、key 文件，ca 文件缺省放置在目录“/milstar 安装目录/cafile”下。客户端 cert、key 文件缺省放置在目录“/milstar 安装目录/cerfile”下。
- 智能卡认证：需要选择分发给用户的 ca 文件，ca 文件缺省放置在目录“/milstar 安装目录/cafile”下，还需选择操作智能卡的动态链接库“aetpkss1.dll”，缺省在目录“/milstar 安装目录”下。选择动态链接库后，需更新智能卡信息。

（4）加密协议：和服务器一致；

（5）数据压缩：和服务器一致。

图 3 配置界面

配置完成后，点击主界面上的“连接”按钮，就可建立与服务器端的安全通道。

3.3 保险箱管理

点击主菜单的管理按钮，进入“保险箱管理”选项页。通过保险箱管理配置，用户可以选择保险箱连接成功后，是否自动打开保险箱界面。界面如图 4 所示。

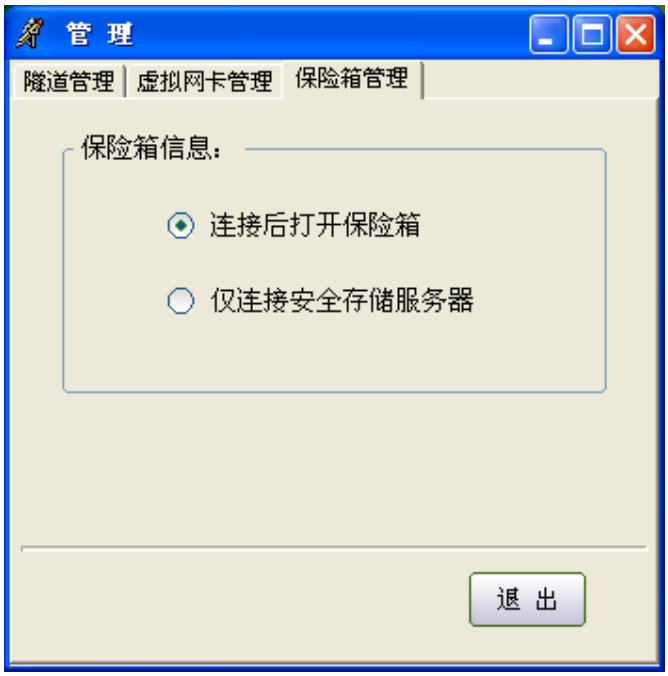

图 4 保险箱选项页

3.4 使用保险箱

3.4.1 连接保险箱

对客户端配置完毕后，便可以连接服务器，打开保险箱。

用户可以直接点击主界面上的“保险箱”，此时 Milstar 会自动建立安全隧道，并连接保险箱。连接成功后的提示界面如图 5 和 6 所示。

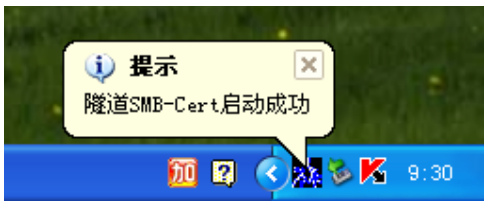

图 5 隧道连接成功提示

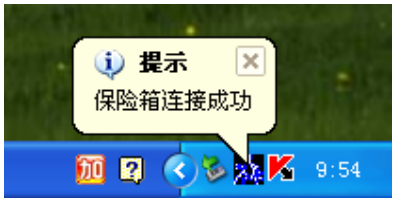

图 6 保险箱连接成功提示

同时在我的电脑中，也可以看到已经连接上的保险箱。如图 7 所示。

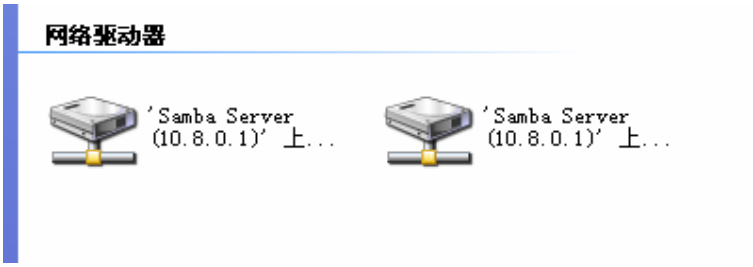

图 7 我的电脑中保险箱

经过上述步骤后，用户可以象访问本地盘一样访问服务器保险箱，服务器保险箱中的数据是加密存储的，保障个人数据的安全性。

3.5 断开保险箱

点击“断开隧道”，保险箱便会自动断开连接，同时我的电脑中的“网络驱动器”也会自动断开。