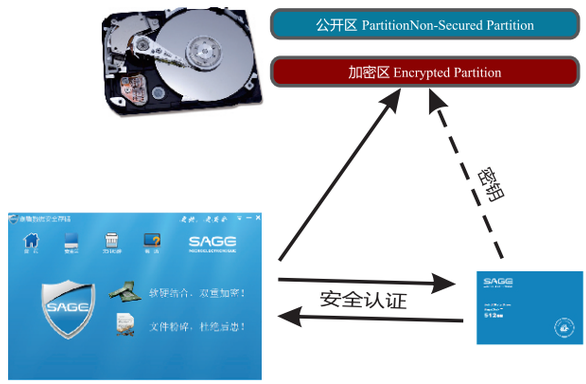
系统应用方案：澜盾™卫士

SSD Solutions：Shield Systems

华澜微澜盾™安全型SSD模块专门为了需要在硬盘实现数据安全功能的系统集成商而开发。华澜微可以配合实现客户定制的安全型固态硬盘产品。客户可以选择加密算法并定义加密认证流程。

安全型SSD模块的主要特色在于提供了硬件数据加密功能和分区功能。针对不同的分区可以采用不同的密钥或者认证过程。同时，每个固态硬盘内的特定序列号或者电子签名内容，可以使得主机、特定软件或者网络服务器识别硬盘本身的特性，从而实现固态硬盘和主机之间、固态硬盘和特定软件之间或者固态硬盘和网络服务器之间的互相身份认证，即互相绑定。



客户根据这些特色技术点，根据自己的需要，应用安全型SSD模块于：

- 主机和硬盘绑定：用户信息只能够限制在特定机器和个人使用范围
- 软件和硬盘绑定：类似硬件狗的特征，可以实现版权保护和软件的授权控制
- 服务器和硬盘绑定：通过网络授权电脑对信息的使用

主要特征
Key Features

- **国产硬件级芯片加密：AES,SHA,DES/3DS,RSA, SM..**
  - 系统采用先进的结构化、模块化设计可根据用户实际需求增加功能模块，扩展性好。所有客户端都是由服务器进行控制，客户端所有权限都可以通过服务器进行设置。提供网络版和单机版两种电脑客户端控制软件
- **硬盘分区功能**
  - 分公开区和加密区；将盘分成CD-ROM区和安全存储区（隐藏），具有只读功能，防止病毒感染
- **通过BIOS口令加载SSD硬盘**
  - Sentinel：BIOS密码启动SSD公开区，BIOS密码不同启动所有分区
  - Mirage：BIOS不同密码启动不同分区，分区之间相互隔离
  - Ranger：通过专用U-KEY启动SSD隐藏区
  - Hermit：BIOS密码启动后通过系统内程序键入密码启动隐藏分区
  - Guard：固态硬盘配合澜盾管理系统，用于管理原有机械硬盘的数据。固态硬盘与澜盾管理系统之间有认证机制，用以启动加密虚拟盘
- **专用加密U盘(含KEY)**
  - 采用国密SM4数据加密、按键密码身份认证、原厂芯片级技术保障的三重安全防护机制，数据安全性高、信任度高
  - 数据自毁和防密码破解功能，原厂也无法破解
  - U盘专用文件系统和专用资源管理器技术：保证U盘数据安全，主动防止病毒感染
  - U盘数据防拷贝技术：防止数据泄密
- **可控自毁功能**

  通过按键、定时销毁，软件指令和远程通信模块等四种方式自毁