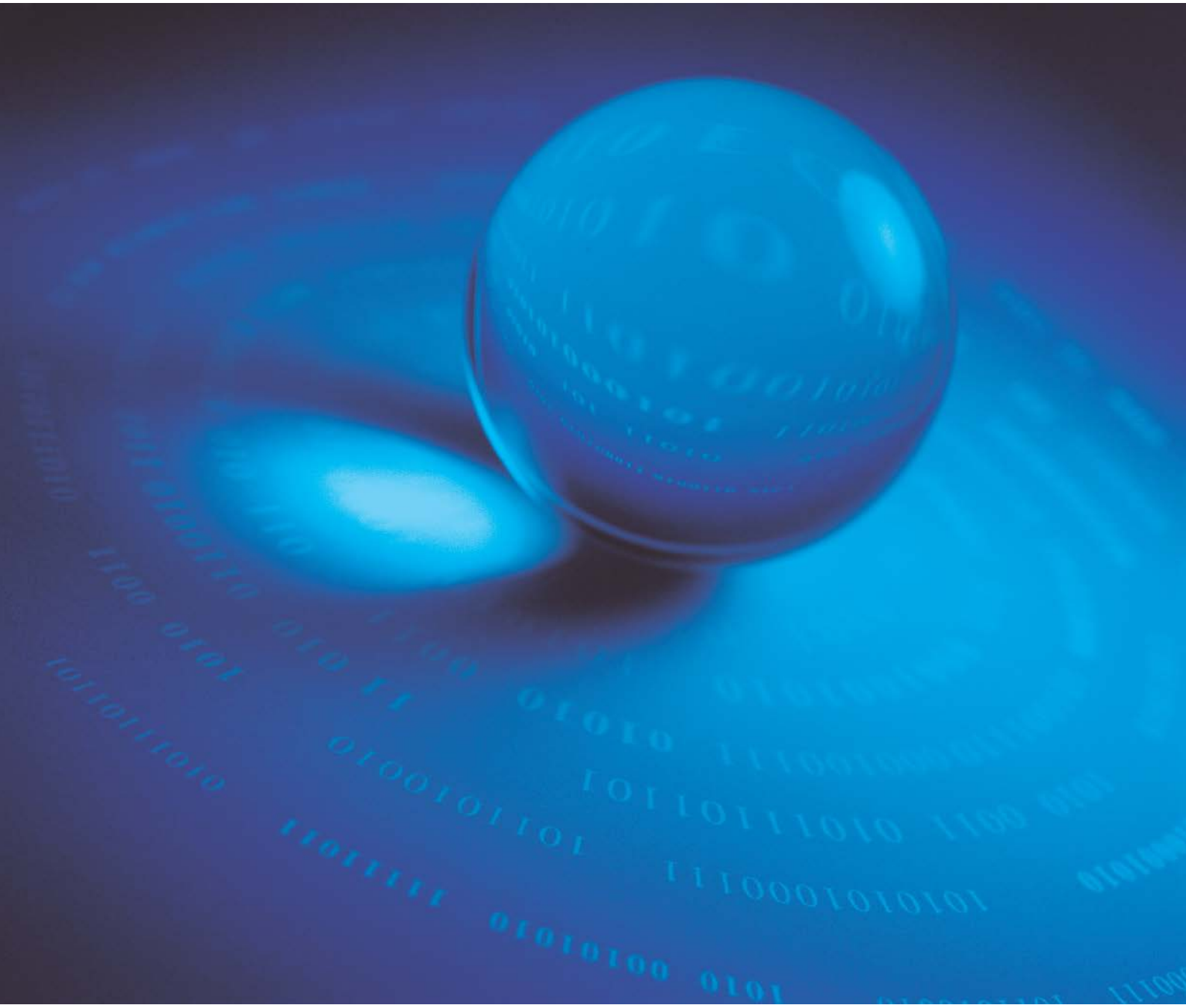
ePass3003 硬件说明

1.2 版



http://www.EnterSafe.com

EnterSafe 尽最大努力使这篇文档中的内容完善且正确。EnterSafe 对于由这篇文档导致的任何形式的直接或间接损失不负有责任。这篇文档的内容会跟随产品的升级而有所变化。

修改记录：

日期	版本	说明
2007 年 1 月	1.0	第一版
2008 年 1 月	1.1	第一版第一次修订
2009 年 5 月	1.2	第一版第一次修订

EnterSafe
软件开发协议

本《软件开发协议》（以下简称《协议》）是用户（个人或者单一机构团体）与 EnterSafe 之间有关随附本《协议》的 EnterSafe 软件产品的法律协议。本软件产品包括计算机软件，并且还可能包括电子文档、相关媒体和印刷材料（以下简称“软件产品”）。您一旦安装、复制或以其他方式使用本“软件产品”，即表示您同意接受本《协议》中的条款的约束。如果您不同意本《协议》中的条款，则您不得安装、复制或以其他方式使用本“软件产品”；您可以将本“软件产品”退还原购买处并取得全额退款。

1.软件产品使用许可

如果您遵守本协议的条款，EnterSafe 将授予您协议中所述的权利。

1.1 EnterSafe 授予您作为个人的、非独家性的许可证，仅供您为用于设计、开发及测试您的设计以及与任何 EnterSafe 产品一起运行的软件产品。您可在无数量限制的计算机上安装本“软件产品”的副本，但您必须是本“软件产品”的唯一使用者。如果您为一个机构团体，EnterSafe 授予您指定您组织内一位人员依以上所规定的方式使用本“软件产品”的权力。

1.2 EnterSafe 允许您将本软件合并或链接到您的计算机程序中，但本软件产品中被合并或链接的部分仍受本协议的约束。

1.3 您可以以存档为目的复制合理数量本软件产品的副本;但如果 Entersafe 通过公开声明或发布新闻的形式终止软件副本的使用，您必须马上遵守这个要求。

2.反向工程、反向编译、反汇编的限制

您不可以对本“软件产品”的部分或全部进行反向工程、反向编译或反汇编；尽管有这项限制，如果适用法律明示允许上述活动，则不在此限制范围。

3.禁止租借、传播或商业主办服务

您不可出租、租赁或出借本“软件产品”；或将本“软件产品”放在服务器上传播；或利用本“软件产品”提供商业主办服务。

4.责任限制和补救措施

无论任何原因（包括但不限于上述所有直接规定或一般性的合同规定或其它情况）发生的损害，EnterSafe 与其供应商在本协议条款下的所承担的全部责任以及全部损害的唯一补偿，不超出您购买本“软件产品”所支付的款额。

5.免责声明

在适用法律所允许的最大范围内，EnterSafe 或其供应商按“现有状况且包含所有错误”提供本“软件产品”或支持服务（如果有），并声明不承担所有其他明示、隐含或法定的担保、责任和条件。其中包括但不限于下列任何担保、责任或条件（如果有）：适销性、对于特定目的的适用性、可靠性或可用

性、回应的准确性或完整性、结果或工艺的精良性、无病毒以及无疏忽；还包括通过本“软件产品”或因使用本“软件产品”而提供或未提供支持服务或其他服务、信息、软件和相关内容。用户对本“软件产品”没有所有权、不受干扰的使用权、不受干扰的占有权、与说明一致或不侵权的任何保证或条件。

6.版权所有

EnterSafe 保留所有本《协议》中未明确授予您的权利，本“软件产品”受版权和其它知识产权法及相关条款的保护。EnterSafe 拥有本“软件产品”的所有权、版权和其他知识产权。

7.协议终止

本《协议》在终止前有效。若您违反本《协议》的任何条款，使用本“软件产品”的权利将自动终止。本“软件产品”必须被销毁或返回 EnterSafe。您可以销毁本“软件产品”及其所有副本以终止协议。但条款 2，3，4，5，6 将继续有效。

CE Attestation of Conformity

The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

FCC certificate of approval

This Device is conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

USB

This equipment is USB based.

WEEE

Dispose in separate collection.

章节目录

第一章 ePass3003 硬件说明

1.1 ePass3003 的优点

ePass3003 采用了一流的工艺制造的智能卡芯片，是保护用户敏感数据的理想设备。其优点包括：

- 无需硬件驱动（HID）

ePass3003 采用 HID 扩展设备技术，利用操作系统内置的标准 HID 驱动实现对 USB Key 的访问。在 Windows 98SE 以上的 Windows 操作系统以及在 Linux 和 Mac OS 等操作系统中使用 ePass3003 无需另外安装硬件驱动，增加了软硬件系统的稳定性。

- 高性能

使用专门定制的高安全 CPU 核心，采用 32 位的处理器，主频更可在高达 96MHz 下稳定工作，并配有硬件加密协处理器。在与高性能 CACHE 共同配合下，使智能卡性能达到最优。

- 高安全性

使用基于硬件 RSA 算法的 ePass3003 比使用单纯的软件实现的 RSA 应用更加安全可靠。因为敏感数据都被安全地保存在 ePass3003 的安全存储区域中，未授权用户是无法接触到这些信息的。数据的签名和加密操作全部在 ePass3003 内部完成，私钥从生成的时刻起就一直保存其中，可有效的杜绝黑客程序的攻击。ePass3003 的安全性还在于 ePass3003 使用的加密算法都是被广泛公开，业界公认的，经受了多年考验的算法。同时，一流的芯片封装工艺也保证了芯片内数据的安全性。

- 灵活易用

使用 ePass3003 无需任何附加的外部设备。用户只要简单的将 ePass3003 插入任何带有 USB 接口的桌面电脑、笔记本、键盘和显示器的 USB 端口中就可以使用 ePass3003。用户不需要关闭计算机或正在运行的程序，使用完毕之后，直接拔下 ePass3003 就可以了。

- 造价低廉

ePass3003 比任何传统的基于硬件的安全系统都节省开支。由于使用 ePass3003 无需任何附加设备，因此很适合大范围的发行。ePass3003 能够提供智能卡设备提供的所有功能，但是不需要智能卡读卡器。

- 便于携带

ePass3003 体积十分小巧，重量很轻。灵巧封装型外壳采用一体化一次成型工艺，十分坚固耐用而且具有防水的功能。用户可以将 ePass3003 穿在钥匙链上随身携带。

- 无缝集成

ePass3003 提供符合业界广泛认可的 PKCS#11 和 Microsoft CryptoAPI 两种标准的接口，任何兼容这两种接口的应用程序都可以立即集成 ePass3003 进行使用。同时，ePass3003 也针对多个第三方的软件产品进行了兼容性优化。此外，ePass3003 内置大容量的安全存储器，可以同时存储多个数字证书和用户私钥及其他数据，也就是说，多个 PKI 应用程序可以共用同一个 ePass3003。

- 高可靠性

ePass3003 使用严格工艺制造，室温下最少擦写次数 EEPROM 为 80 万次，FLASH 为 2 万次，室温下数据保持时间最少 100 年，有效地确保非易失性存储区可长期安全的保存用户的数据。

1.2ePass3003 的硬件特性

- 标准 HID 设备

ePass3003 使用操作系统提供的 HID 驱动，无需额外安装厂家硬件驱动。

- 高性能的处理芯片

ePass3003 采用高速的 32 位 RISC（精简指令集）处理器的安全 SOC 芯片，具备高处理能力、高安全性、低成本等特点。SOC（System On Chip）是指 CPU 核以及外设（含定时器、各种存储器、各种模拟和数字的接口等等)高度集成在一起的一种单芯片计算系统。

- 硬件实现的加密算法

ePass3003 采用先进的智能卡技术，智能卡芯片内部可实现下列算法：

- 512、1024、2048 位的 RSA 非对称密钥对生成、加解密和签名、校验操作
- 对称加密算法 DES、3DES
- 散列函数 SHA-1

由于关键的加密算法都在硬件内实现，这就保证了进行加密运算的密钥的安全性。

- 硬件 RSA 密钥对生成

ePass3003 的 RSA 密钥对在硬件内部实时生成。用于生成密钥的大素数依靠硬件真随机数发生器产生。

- 硬件随机数发生器

ePass3003 内置硬件真随机数发生器。ePass3003 在内部使用这个随机数发生器进行密钥对生成，以及随机消息鉴别码的生成等操作。

- 片内安全存储区域

ePass3003 的数据存储区（FLASH+EEPROM）、固件存储区（FLASH）及运算部件全部集成在一块芯片内，保证了数据存储的安全。

1.3ePass3003 的硬件技术参数

工作电压	5V（USB 口供电）
工作电流	80-150mA
工作温度	0～70℃
存储温度	-20～85℃
湿度	0~100％不结露
外壳	ABS（树脂）
通讯协议	USB，HID
接口类型	标准 USB1.1 设备 兼容 USB2.0 接口（A 型插头）
处理器	32 位智能卡芯片
存储空间	64K（无国密算法）/60K（带国密 SSF33 算法）/52K（带国密 SCB2 算法）

擦写次数	室温下最少擦写次数 EEPROM 为 80 万次，FLASH 为 2 万次
数据存储年限	室温下数据保持时间最少 100 年
证书和标准	PKCS # 11 v2.20, MS CAPI, X.509 v3 证书存储，SSL v3, IPSec，兼容 ISO 7816，符合 CE 和 FCC 标准
内置安全算法	RSA, DES, 3DES, AES, ECC, SHA-1, SHA-256
芯片安全水平	安全加密的数据存储
支持的操作系统	Windows 2000/XP/XP-64/2003/2003-64/Vista/Vista-64/2008/2008-64/7/7-64/8/8-64，Mac OS，Linux（Mac OS/Linux 仅硬件支持）

*国密算法是指国家密码局指定中国大陆金融交易中使用的算法，包括国密 SSF33 算法和 SCB2 算法。