ePass3000 硬件说明

1.2 版

北京飞天诚信科技有限公司（以下简称“飞天公司”）尽最大努力使这篇文档中的内容完善且正确。飞天公司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	修改
2005 年 6 月 15 日	1.0	第一版
2007 年 8 月 13 日	1.1	第一版第一次修订
2009 年 6 月 2 日	1.2	第一版第二次修订

北京飞天诚信科技有限公司

软件开发协议

北京飞天诚信科技有限公司（以下简称“飞天”）的所有产品，包括但不限于：开发工具包，磁盘，光盘，硬件设备和文档，以及未来的所有定单都受本协议的制约。如果您不愿接受这些条款，请在收到后的 7 天内将开发工具包寄回飞天，预付邮资和保险。我们会把货款退还给您，但要扣除运费和适当的手续费。

1. 许可使用

您可以将本软件合并、连接到您的计算机程序中，但其目的只是如开发指南中描述的那样保护该程序。您可以以存档为目的复制合理数量的拷贝。

2. 禁止使用

除在条款 1 中特别允许的之外，不得复制、反向工程、反汇编、反编译、修改、增加、改进软件、ePass 系列硬件和产品的其它部分。禁止对软件和产品的任何部分进行反向工程，或企图推导软件的源代码。禁止使用产品中的磁性或光学介质来传递、存储非本产品的原始程序或由飞天提供的产品升级的任何数据。禁止将软件放在服务器上传播。

3. 有限担保

飞天保证在自产品交给您之日起的 12 个月内，在正常的使用情况下，ePass 系列硬件和软件存储介质没有重大的工艺和材料上的缺陷。

4. 修理限度

当根据本协议提出索赔时，飞天唯一的责任就是根据飞天的选择，免费进行替换或维修。飞天对更换后的任何产品部件都享有所有权。

保修索赔单必须在担保期内写好，或发生故障 14 天内连同令人信服的证据交给飞天。当将产品返还给飞天或飞天的授权代理商时，须预付运费和保险。

除了在本协议中保证的担保之外，飞天不再提供特别的或隐含的担保，也不再对本协议中所描述的产品负责，包括它们的质量，性能和对某一特定目的的适应性。

5. 责任限度

不管因为什么原因，不管是因合同中的规定还是由于刑事的原因，包括疏忽的原因，而使您及任何一方受到了损失，由我方产品所造成的损失或该产品是起诉的原因或与起诉有间接关系，飞天对您及任何一方所承担的全部责任不超出您购买该产品所支付的货款。在任何情况下，飞天对于由于您不履行责任所导致的损失，或对于数据、利润、储蓄或其它的后续的和偶然的损失，即使飞天被建议有这种损失的可能性，或您根据第 3 方的索赔而提出的任何索赔均不负责任。

6. 协议终止

当您不能遵守本协议所规定的条款时，将终止您的许可和本协议。但条款 2，3，4，5 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 report No. 70407310011
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.

ePass3000 硬件说明

1. ePass3000 的优点

ePass3000 采用了一流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：

- **高性能**

  使用专门定制的高安全 CPU 核心，采用 32 位的 RISC，主频更可在高达 100MHz 下稳定工作，并配有硬件乘法协处理器。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 ePass3000 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 ePass3000 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 ePass3000 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。ePass3000 的安全性还在于 ePass3000 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 ePass3000 无需任何附加的外部设备。用户只要简单的将 ePass3000 插入任何带有 USB 接口的桌面电脑、笔记本、键盘、显示器的 USB 端口中就可以使用 ePass3000。用户不需要关闭计算机或关闭正在运行的程序。使用完毕之后，直接拔下 ePass3000 就可以了。

- **造价低廉**

  ePass3000 比任何传统的基于硬件的安全系统都节省开支。由于使用 ePass3000 无需任何附加设备，因此很适合大范围的发行。ePass3000 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**

  ePass3000 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 ePass3000 穿在钥匙链上，随身携带。

- **无缝集成**

  ePass3000 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 ePass3000 进行使用。同时，ePass3000 也针对多个第三方的软件产品进行了兼容性优化。此外，ePass3000 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 ePass3000。

- **高可靠性**

  ePass3000 使用严格工艺制造，可进行单字节或多字节的擦除、写操作，最少擦写次数 EEPROM 为 10 万次，Flash 为 2 万次，室温下数据保持时间最少 100 年，有效的确保非易失性存储区可长期安全的保存用户的数据。

2. ePass3000 的硬件特性

- **高性能的处理芯片**

  ePass3000 采用高速的 32 位 RISC 处理器的高安全 SOC 芯片，具备高处理能力、高安全性、低功耗、低成本等特点。SOC（System On Chip）是指 CPU 核以及外设（Peripheral：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**

  ePass3000 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 非对称加密算法和签名、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**

  ePass3000 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**

  ePass3000 内置硬件真随机数发生器。ePass3000 在内部使用这个随机数发生器进行密钥对生成，随机消息鉴别码的生成等操作。

- **多级访问权限**

  ePass3000 的文件系统具有多达 16 级的安全权限级别。用户可以定义一个或多个密钥管理安全权级。用户可以根据应用的需要定义出复杂的安全权级关系。

- **片内安全存储区域**

  ePass3000 的数据存储区（RAM）、文件存储区（EEPROM/Flash）、固件存储区（Flash ROM）及运算部件全都集成在一块芯片内，保证了数据存储的安全。

3. ePass3000 技术参数

支持的操作系统	Windows 2000/XP/XP-64/2003/2003-64/Vista/Vista-64/ 2008/2008-64/7/7-64, Linux, Mac OS
证书和标准	PKCS # 11 v2.11, MS CAPI, PC/SC, X.509 v3 证书存储，SSL v3, IPSec, 兼容 ISO 7816
处理器	32 位
存储空间	用户最大 64K
内置安全算法	RSA, DES, 3DES, SHA-1

芯片安全水平	安全加密的数据存储
功率	< 250 mW
工作温度	0 ～ 70° C
存放温度	- 20 ～ 85° C
湿度	0 ～ 100%不结露
接口类型	标准 USB1.1 设备，兼容 USB2.0 接口（A 型插头）
外壳	一次性，防水，硬塑料外壳
数据存储年限	室温下数据保持时间最少 100 年
最少擦写次数	EEPROM：10 万次，Flash：2 万次