ePass3000 的 Word 应用

1.2 版

www.FTsafe.com

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.

缩略语及术语

缩略语及术语	解释
PKCS#11 接口	由 RSA(www.rsasecurity.com)实验室推出的程序设计接口，将密码设备抽象成一种通用的逻辑视图即密码令牌（Cryptographic Token）提供给上层应用，做到设备无关性和资源共享。
CryptoAPI 接口(简称 CAPI)	由微软公司提供的密码(cryptography)操作接口，提供设备无关的或软件实现的密码算法封装，很容易使开发者能够开发出用于数据加解密、使用数字证书的身份认证、代码签名等的 Windows 平台上的 PKI 应用程序。
Token	密码设备的统称，可以是智能卡，也可以是具有密码和证书存储功能的任何设备。
USB Token	具有 USB 接口的密码设备，其携带方便，操作简单。
ePass3000	飞天公司推出的将智能卡和 USB 接口结合的便携式设备，具有智能卡的优点，又有携带方便的好处。支持 PKI 应用。
ePassNG (ePass Next Generation)	飞天公司推出的新一代的中间件框架产品，支持 ePass 系列等产品，并能够非常方便的增加被支持的硬件。支持 PKI 应用。

目　录

第一章 ePass3000 的Word应用指南

ePass3000 的设计目标之一就是与现有的 PKI 体系应用无缝的集成。PKI 应用开发商无需对 ePass3000 进行任何形式的编程开发就能通过配置相关服务而可以将 ePass3000 集成于 PKI 应用当中。

目前支持 PKI 的应用有些使用 PKCS#11 接口，有些使用 Crypto API（简称 CAPI）接口，后者都是微软的 Windows 平台下的应用，而前者在任何平台下都有。

本章主要讲述如何配置 ePass3000 的 Word 应用。本手册包括使用 ePass3000 对 Word 文档进行签名和加解密的操作方法。

- 使用 ePass3000 对 Word 文档进行签名
- 使用 ePass3000 对 Word 文档进行加密
- 访问使用 ePass3000 加密过的文档

首先安装好 Microsoft Office Word，本手册以中文 Word2003 为例进行说明。同时安装好 ePass3000 的 Runtime 包。

1.1 使用ePass3000 对Word文档进行签名

1. 确保ePass3000 已经申请过证书，证书申请的方法请参见ePass3000 的CAPI应用指南和ePass3000 的Netscape应用指南。用Microsoft Office Word 2003 打开/编辑一个Word文档，选择菜单项“工具”—〉“选项”，如图 1所示：

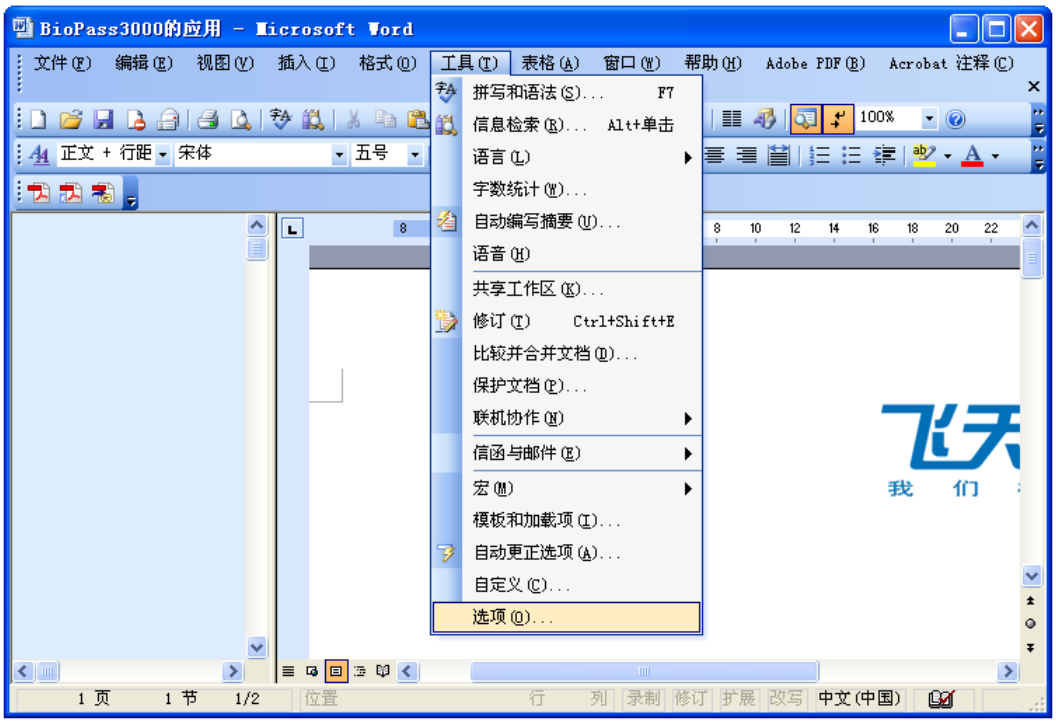

图 1 选项菜单

2. 弹出“选项”对话框，选择“安全性”选项卡，如图 2所示：

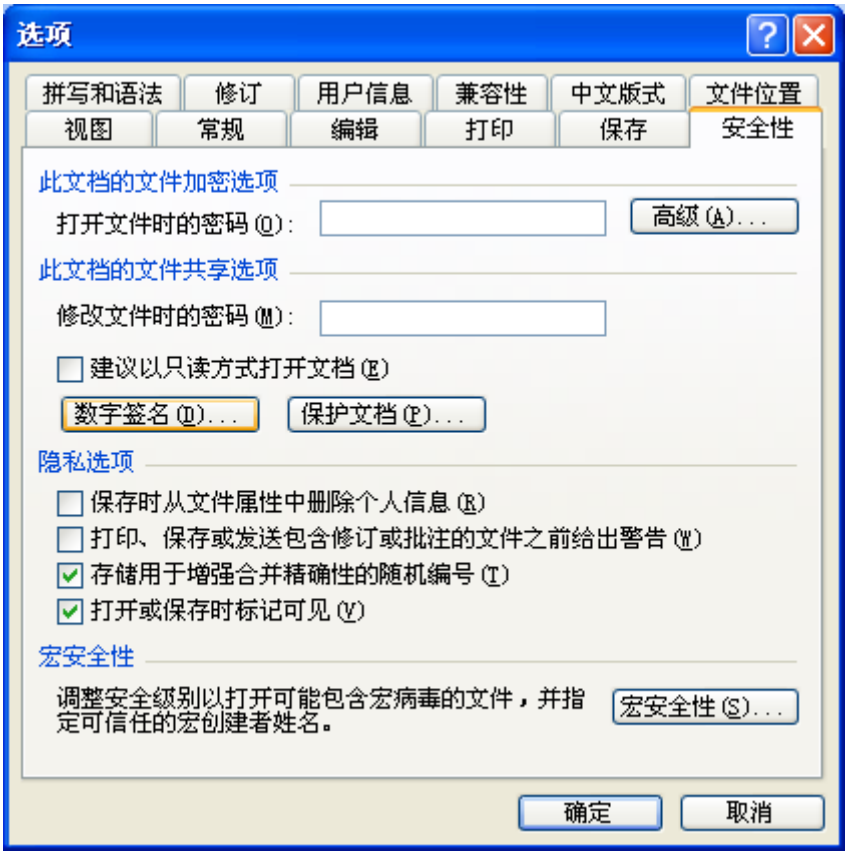

图 2 安全性界面

3. 点击“数字签名”按钮，弹出如图 3所示的“数字签名”对话框：

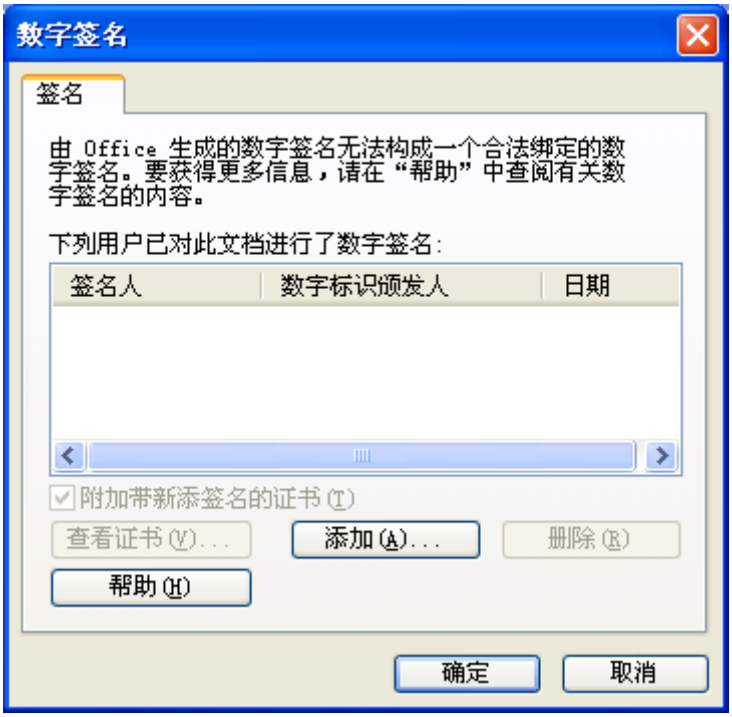

图 3 数字签名对话框

4. 点击“添加”按钮，弹出“选择证书”对话框，如图 4所示：

图 4 选择证书对话框

5. 在证书列表中选择ePass3000 内的证书，然后点击“确定”按钮，此时会弹出如图 5所示的PIN 码输入框：

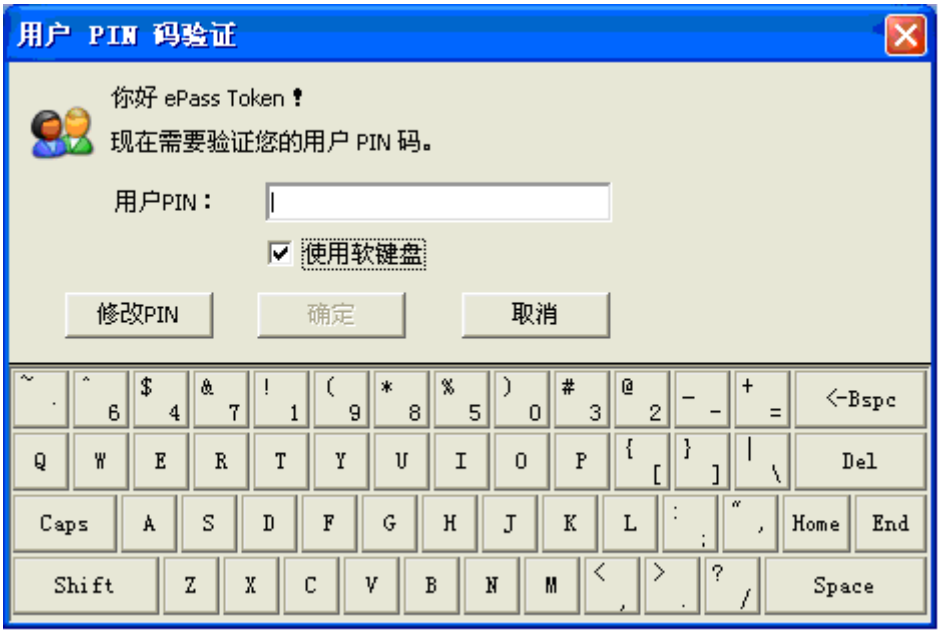

图 5 PIN 码输入框

注意：上图显示的是使用软键盘输入用户 PIN 码的情况，用户可以不选择“使用软键盘”选项，但是建议您选择“使用软键盘”登录到 Token，这样才能保证您的 PIN 码的安全。选择“使用软键盘”后，物理键盘被禁用。

如果用户想修改 PIN 码，可以按照步骤 6 的说明进行操作，如果不需要修改 PIN 码，直接执行步骤 8。

6. 点击图 5所示界面中的“修改PIN”按钮进行用户PIN码的修改，点击“修改PIN”弹出如图 6所示的对话框：

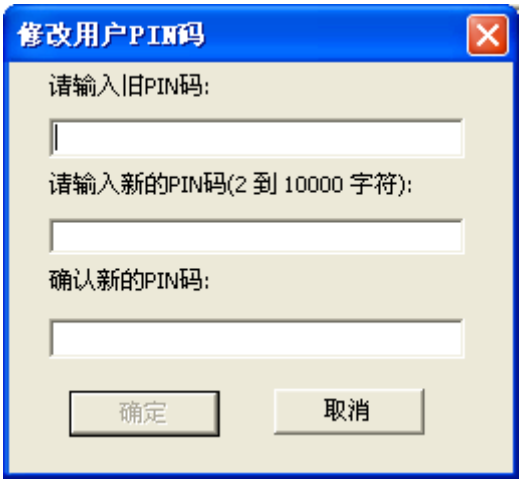

图 6 修改 PIN 码对话框

7. 按照界面上的要求输入原PIN码和新PIN码并确认，然后点击“确定”按钮，完成用户PIN码的修改。修改PIN码后ePass3000 自动登录，无须再进行PIN码验证，此时可以看到如图 7所示的对话框。

8. 输入正确的PIN码后点击“确定”按钮，选择的ePass3000 内的证书就被添加到签名证书列表中了，如图 7所示：

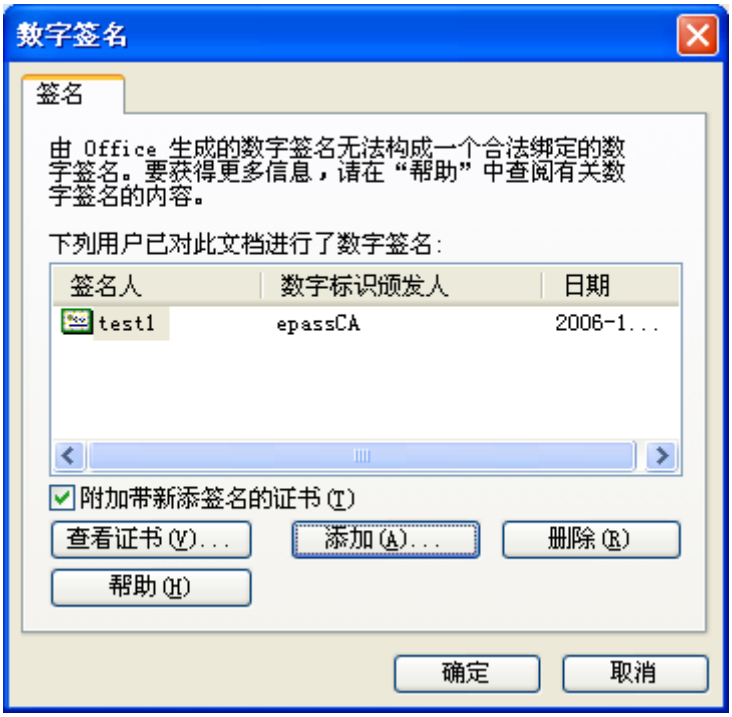

图 7 签名证书列表

9. 点击“确定”按钮关闭“数字签名”对话框，再点击“确定”按钮关闭“选项”对话框，完成对Word文档的签名。在签名后的Word文档下方的状态栏处出现一红色的签名图标，当鼠标滑过此图标时显示“此文档已被数字签名”的提示，如图 8所示：

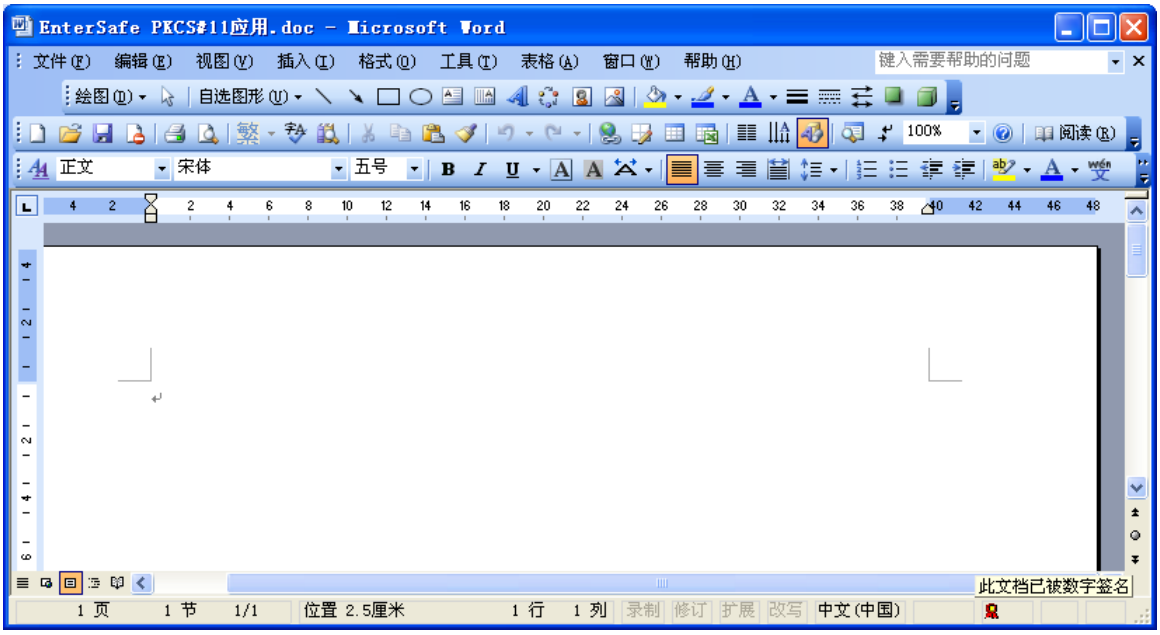

图 8 签名后的文档

10. 双击状态栏上的签名图标，弹出如图 7所示的数字签名对话框，您可以点击“查看证书”按钮，查看证书的详细内容。

注意：当您打开一个签名过的文档时在 Word 文档的标题栏内的标题中显示“已签名，未验证”，如果您进行步骤 8 的操作后，“已签名，未验证”消失，表明您已经验证过该文档。

11. 如果您对文档进行修改，点击保存按钮会弹出删除签名对话框，如图 9所示：

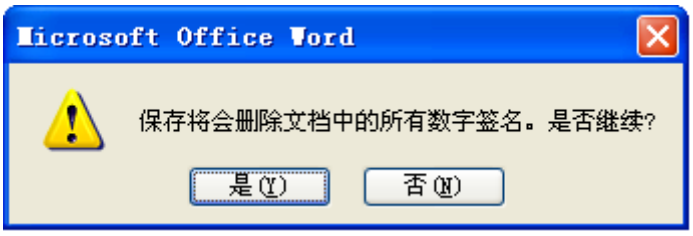

图 9 提示删除数字签名对话框

12. 点击“是”按钮，保存对文档的修改，并删除原有的数字签名。此时您可以看到状态栏上的签名图标和标题栏上的“已签名”消失。这表明此 Word 文档不再有数字签名来证明其真实有效。只有再次对文档进行签名才能证明其真实有效。

13. 如果修改了Word文档的内容，但还未点击保存按钮，当您双击状态栏上的签名图标时，弹出“数字签名”对话框，在签名证书列表中您可以看到签名人前边的图标变为不可信任状态，这表明此文档已经被修改过，该签名证书对文档的签名不能证明其真实有效，如图 10所示：

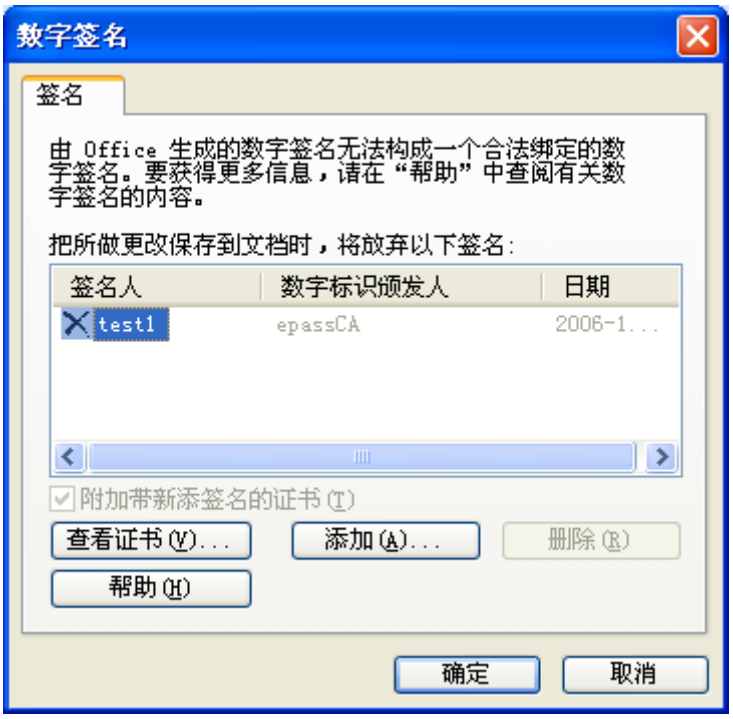

图 10 签名证书列表

注意：Word 文档可以使用多个数字证书对其进行签名，这表明可以由多人共同证明 Word 文档的真实有效。

14. 采用上述同样的方法利用另一个证书（此证书可以是存储于另外一个Token内的证书或存储于Windows系统内的证书）对文档进行签名，签名证书列表如图 11所示：

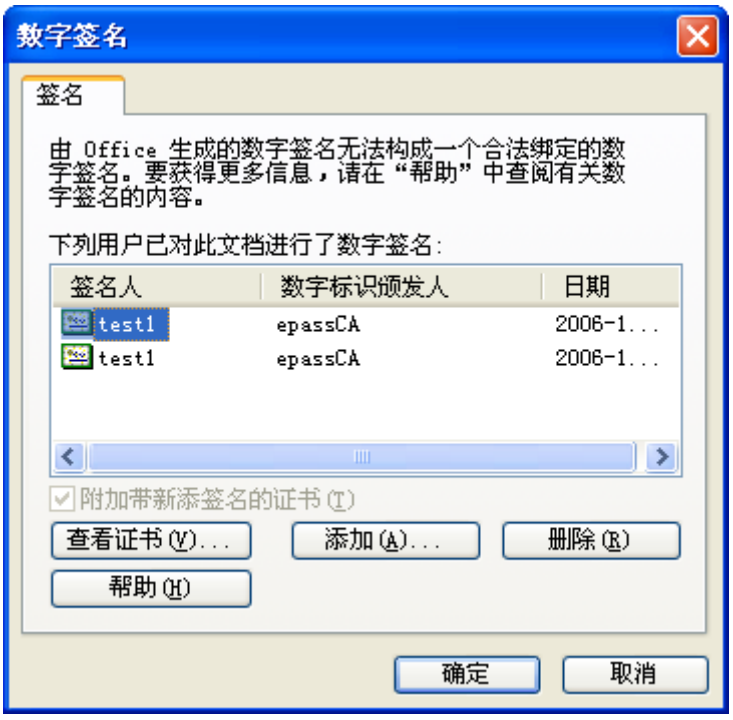

图 11 签名证书列表

1.2 使用ePass3000 对Word文档进行加密

1. 用Microsoft Office Word 2003 打开/编辑一个Word文档，选择菜单项“工具”—〉“选项”，如图 1所示。

2. 弹出“选项”对话框，选择“安全性”选项卡，如图 2所示。

注意：加密 Word 文档时至少插入一把 ePass3000，并且这把 ePass3000 内必须有证书，当插入多把 ePass3000 时只能有一把 ePass3000 内有证书。

3. 点击“高级”按钮，弹出“加密类型”对话框，如图 12所示：

图 12 选择加密类型对话框

4. 选择 RC4，FEITIAN ePassNG RSA Cryptographic Service Provider 加密类型，根据需要选择密钥的长度，根据需要并选择“加密文档属性”复选框，点击“确定”按钮。

5. 在“选项”对话框“打开文件时的密码”的密码框中输入密码，如图 13所示：

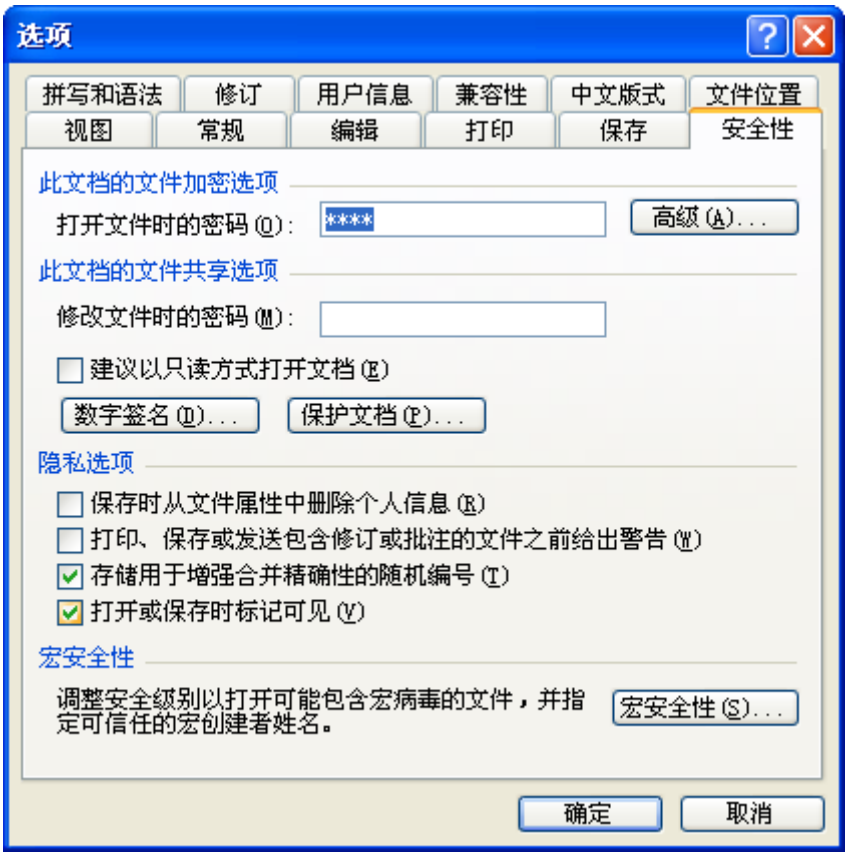

图 13 输入打开文件时的密码

6. 点击“确定”按钮，弹出“确认密码”对话框，如图 14所示，再次输入密码后点击“确定”按钮即完成对Word文档的加密。

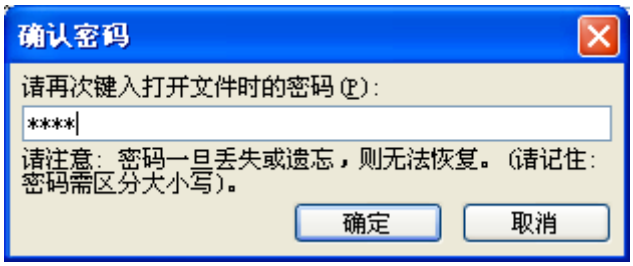

图 14 确认密码对话框

7. 保存文档，同时也保存了对文档的加密操作。

1.3 使用ePass3000 访问加密过的文档

如果您在计算机的 USB 接口上插入了 ePassNG 系列的锁，打开 Word 文档，在弹出的密码输入框中输入正确的密码即可将加密的 Word 文档解密。

如果没有插入锁，即使在弹出的密码输入框内输入了正确的密码，也无法打开加密的Word文档，如图15所示：

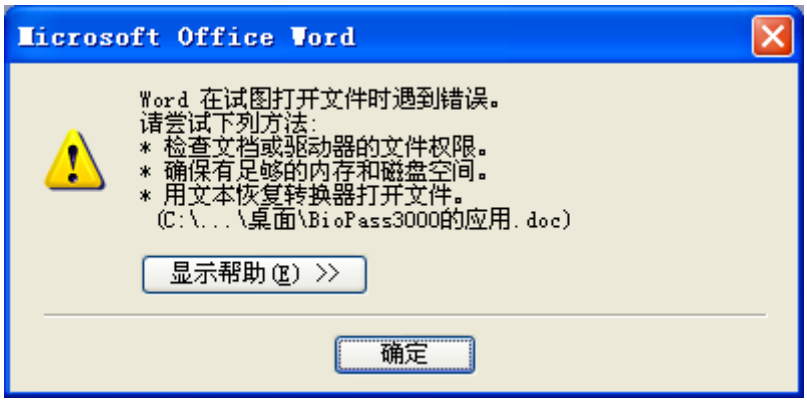

图 15 无法打开 Word 文档