

ET199 的 Word 应用

1.1 版



版权所有©2007-2008 EnterSafe

<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

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以任何 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 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.

章节目录

第一章 ET199 的Word应用指南	1
1.1 使用ET199 对Word文档进行签名.....	1
1.2 使用ET199 对Word文档进行加密.....	5
1.3 使用ET199 访问加密过的文档	7
附录 缩略语及术语	8

图目录

图 1 选项菜单	1
图 2 安全性界面	2
图 3 数字签名对话框	2
图 4 选择证书对话框	3
图 5 登录ET199	3
图 6 签名证书列表	4
图 7 签名后的文档	4
图 8 提示删除数字签名对话框	4
图 9 签名证书列表	5
图 10 签名证书列表	5
图 11 选择加密类型对话框	6
图 12 输入打开文件时的密码	6
图 13 确认密码对话框	7
图 14 无法打开Word文档	7

第一章 ET199 的 Word 应用指南

ET199 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 ET199 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 ET199 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 CryptoAPI（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 ET199 的 Word 应用。本手册包括使用 ET199 对 Word 文档进行签名和加解密的操作方法。

- 使用 ET199 对 Word 文档进行签名
- 使用 ET199 对 Word 文档进行加密
- 访问使用 ET199 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 ET199 的 Runtime 包。

1.1 使用 ET199 对 Word 文档进行签名

1. 确保ET199已经申请过证书，证书申请的方法请参见ET199的CAPI应用指南和ET199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：

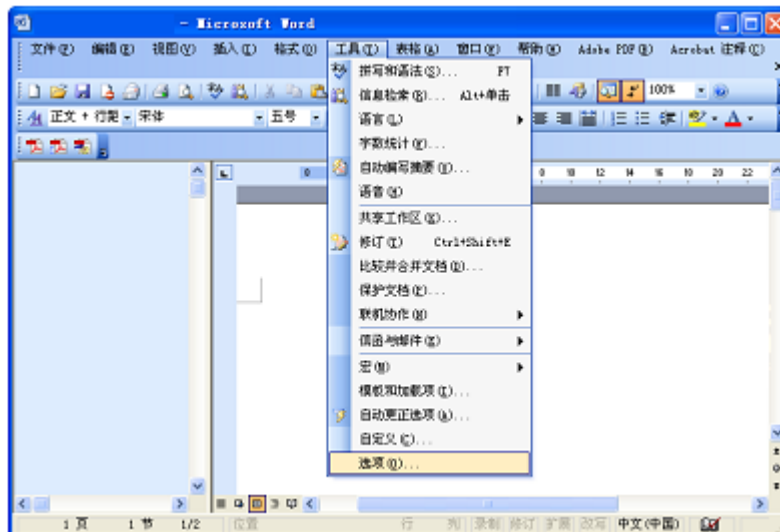


图 1 选项菜单

2. 弹出“选项”对话框，选择“安全性”选项卡，如图 2所示：

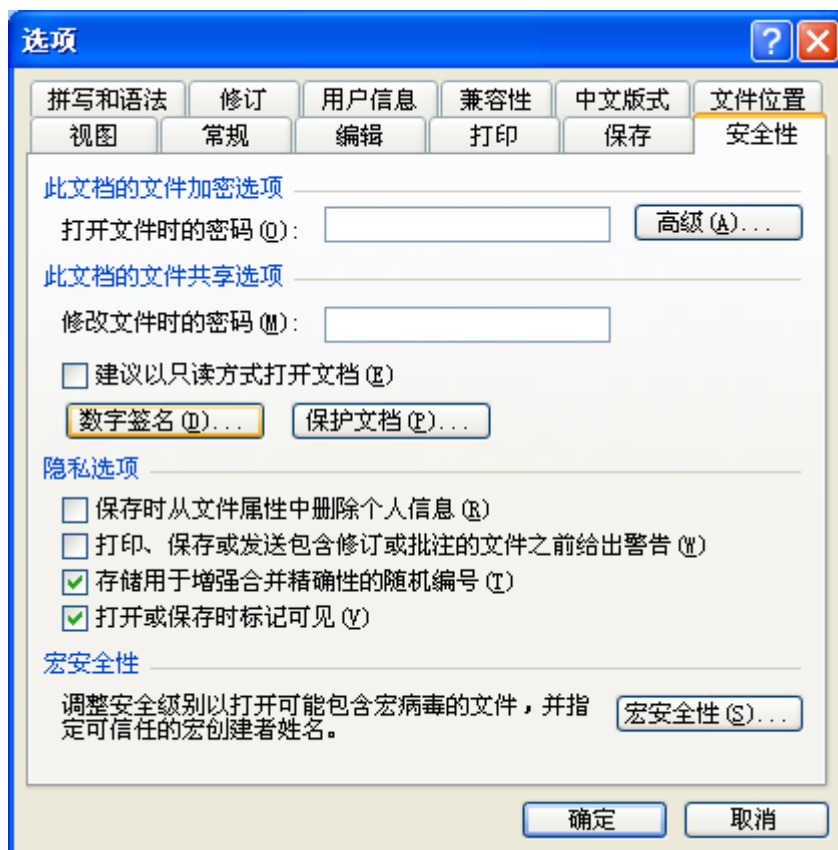


图 2 安全性界面

3. 点击“数字签名”按钮，弹出如图 3所示的“数字签名”对话框：

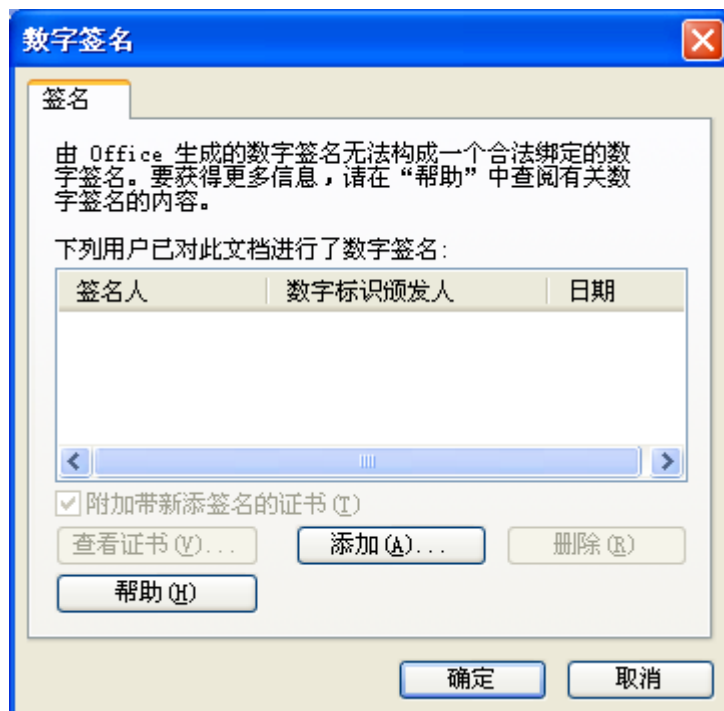


图 3 数字签名对话框

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ET199 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：

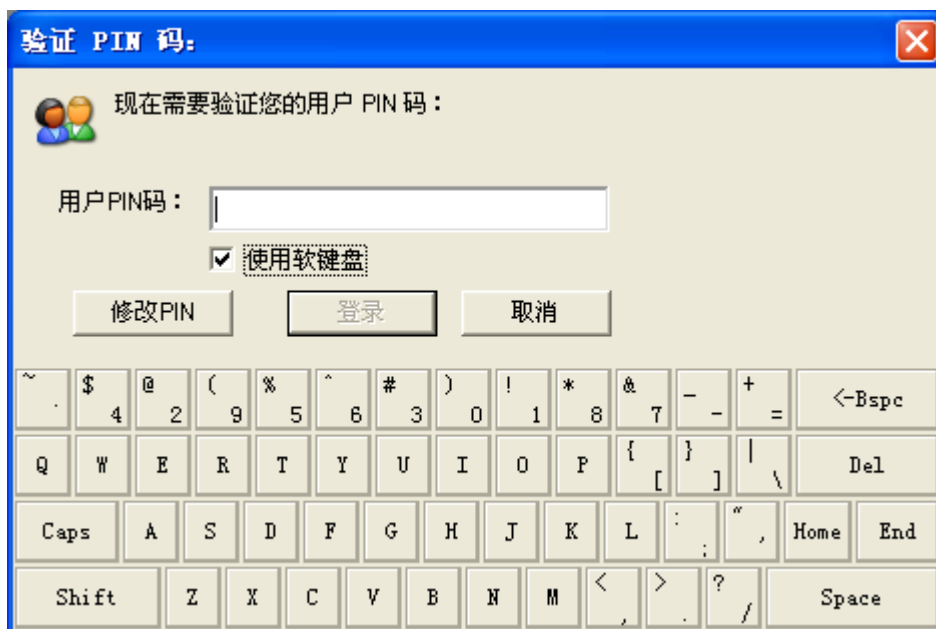


图 5 登录 ET199

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，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，物理键盘的键盘输入将被禁用。另外，只有 Windows2000 以上的操作系统支持软键盘功能，Windows Me 和 Windows98 没有此功能。

用户可以点击“修改 PIN”按钮弹出修改 PIN 码对话框，进行 PIN 码修改。

6. 输入正确的PIN码后点击“登录”按钮，选择的ET199 内的证书就被添加到签名证书列表中了，如图 6所示：



图 6 签名证书列表

7. 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 7所示：

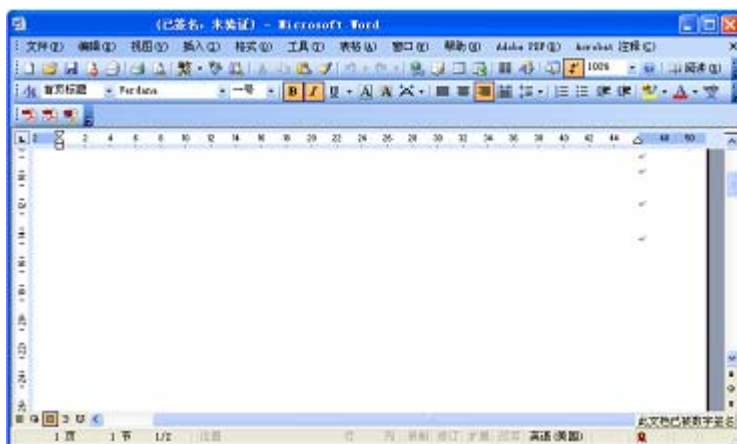


图 7 签名后的文档

8. 双击状态栏上的签名图标，弹出如图 6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。

9. 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 8所示：

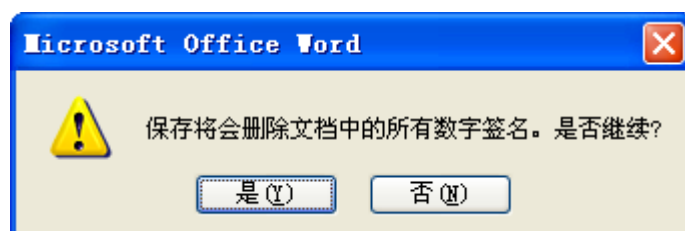


图 8 提示删除数字签名对话框

10. 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。

11. 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 9所示:



图 9 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。

12. 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 10所示:



图 10 签名证书列表

1.2 使用 ET199 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. 将 ET199 插入计算机。

注意：加密 Word 文档时至少插入一把 ET199，并且这把 ET199 内必须有证书，当插入多把 ET199 时只能有一把 ET199 内有证书。

3. 弹出“选项”对话框，选择“安全性”选项卡，如图 2 所示。

4. 点击“高级”按钮，弹出“加密类型”对话框，如图 11 所示：

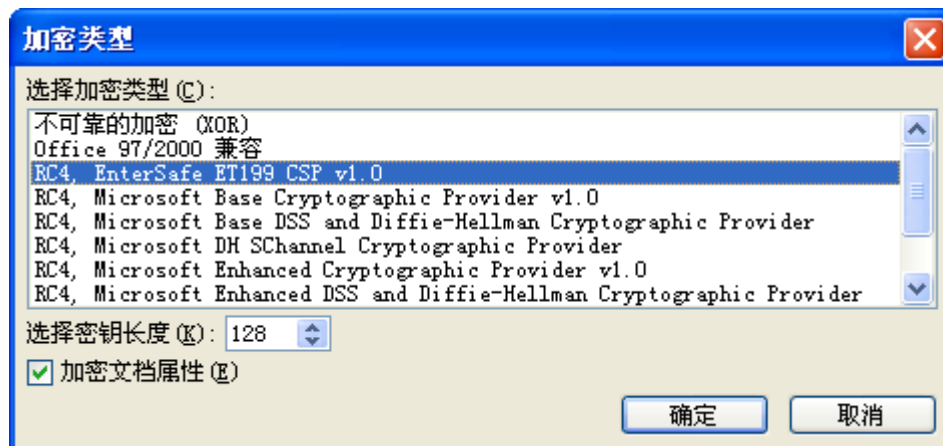


图 11 选择加密类型对话框

5. 选择 RC4, EnterSafe ET199 CSP v1.0 加密类型，根据需要选择密钥的长度，根据需要选择“加密文档属性”复选框，点击“确定”按钮。

6. 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 12 所示：

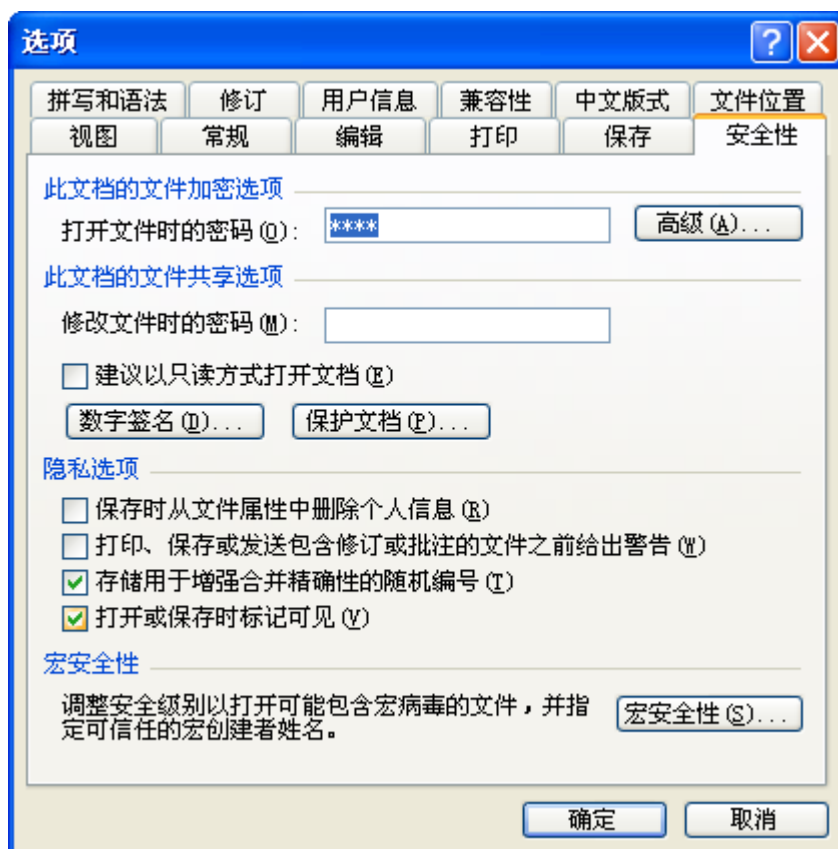


图 12 输入打开文件时的密码

7. 点击“确定”按钮，弹出“确认密码”对话框，如图 13 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。

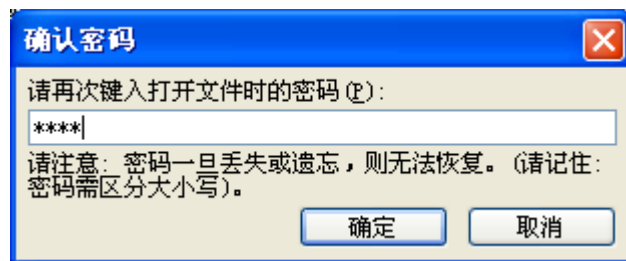


图 13 确认密码对话框

8. 保存文档，同时也保存了对文档的加密操作。

1.3 使用 ET199 访问加密过的文档

如果您在计算机的 USB 接口上插入了加密时使用的 ET199，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。

如果没有插入加密时使用的 ET199，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 14 所示：

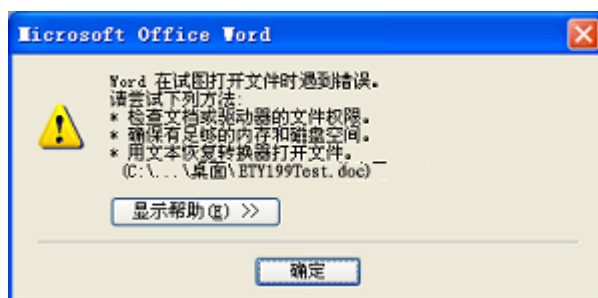


图 14 无法打开 Word 文档

附录 缩略语及术语

缩略语及术语	解 释
ET199	坚石诚信推出的 USB 接口的便携式密码设备，具有高性能、高安全性、灵活易用、造价低廉、携带方便等好处。
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硬件设备。
USB Token	具有 USB 接口的密码设备，其携带方便，操作简单。ET199 是其中一种。
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。
PKCS#11 接口	由 RSA 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。