SafeNet

eToken 双因素身份认证解决方案

上海旺财信息技术有限公司

2009 年 12 月

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

目　　录

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室　(200233)
电话：8621-64701090　　传真：8621-54640133-803
E-mail：jackwrw@msn.com　网址：http://www.wang-cai.com
免费电话：400-600-9103

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

1 SafeNet 公司简介

SafeNet 成立于 1983 年, 为全球知名网络安全整体解决方案提供商，除了不断研发最新信息安全技术外，我们为客户提供双因素身份认证、数据加密和密钥管理及软件版权管理等专业解决方案。

SafeNet 总部设于美国巴尔的摩市，在安全网络系统开发、设置、管理等专业领域有超过 20 年的经验，为政府部门、金融机构及全球大型企业提供专业的产品及服务。SafeNet 在下列各领域皆扮演重要的领导地位: 远程安全登陆客户端标准软件设置；取代用户名/密码的 USB 硬件身份认证令牌；加速 SSL 加解密运算的 SSL 加速装置；防堵非法盗版的软件保护及授权解决方案；及提供给美国政府国防部、国家安全局的高安全加解密系列产品。

SafeNet 在 2004 年 3 月完成与 Rainbow 公司的合并，正式跻身为全球最大、最完整的信息安全产品技术供货商。

2009 年 3 月，阿拉丁知识系统公司被私人投资公司 Vector Capital 收购并且并入其全资子公司 SafeNet。SafeNet 与阿拉丁的合并组成一个软件版权管理（SRM）和身份认证解决方案的全球领导者。两家公司已经引入革新技术在这些领域中，所以这是一次真正的领导者的联合，两家公司在市场上的革新技术能够服务于彼此的客户。两个公司的产品能够充分融合实现最大的市场价值。

SafeNet 积极将专业的产品及技术推广至政府部门、金融机构、企业、OEM 客户及所有需要服务的客户。SafeNet 在全球为 5,000 家客户提供专业的支持及服务，并在全世界 100 个以上的国家拥有广泛的经销渠道。

2 技术及产品线

身份及存取管理- SafeNet 提供形式多样并且独具技术创新的强身份认证解决方案，加强数据存取的安全性，保护用户身份，确保满足合规需求，快速开拓新的业务机会。通过一个强大的可扩展的管理平台以及包括 USB 智能卡认证设备、易于布署的一次性密码解决方案、适用于数字签名和统一物理/逻辑访问的专有产品，SafeNet 提供形式多样的、易于扩展的和极度灵活的身份和存取管理。

磁盘和文件加密- SafeNet 提供磁盘、文件和移动介质最安全和有效的数据保护。SafeNet 的磁盘和文件加密解决方案通过强加密来解决公司笔记本电脑和移动存储介质上敏感数据的安全性需求。SafeNet 解决方案使企业和政府机构不仅布署业界最值得信任的安全，而且充分利用现有的诸如微软活动目录等集中管理系统来降低采购成本。

数据库和应用程序加密- SafeNet DataSecure 是业界最安全、布署最快速并且最容易管理的企业数据库和应用程序保护解决方案。使用 SafeNet DataSecure，企业能够保护关键数据防止来自于内部和外部的威胁，确保满足法规对安全的强制需求，降低数据被窃取的风险。

高速网络加密- SafeNet 高速网络加密设备集合了最高的性能以及最容易的集成和管理来有效保护高速广域网上传输的数据。SafeNet 加密设备提供最快最简单的方式集成强大的 FIPS 认证的网络安全来保护关键的业务数据。千兆级别的输出以及最低的网络延迟使 SafeNet 的加密设备成为保护大容量数据传送理想的解决方案。

硬件安全模块（HSM）- SafeNet 硬件安全模块是博阿虎加密密钥、身份、应用程序和交易最快、最安全、最容易集成的解决方案。通过保护任何以加密为基础的安全解决方案的核心部分——加密密钥，SafeNet 硬件安全模块提供密钥可靠的保护防止泄露，确保满足合规需求，降低法律责任的风险并且提升盈利能力。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

3 eToken 产品介绍

eToken 提供一套完整的安全解决方案，来满足所有认证要求（访问网络、访问 VPN 和 Web 服务器），并保障笔记本电脑和计算机文件的安全。在企业组织中，通过令牌管理系统(TMS)，以 Active Directory®为基础，可以轻松地对令牌进行分配、调度及个性化管理。

3.1 eToken TMS（令牌管理系统）

SafeNet 的令牌管理系统，是一个健壮的管理系统。能够部署、供应和维护所有的 eToken 设备，包括 USB 设备、智能卡和 ID 证章。它支持大量的安全应用程序，例如：网络登录、VPN、Web 访问、一次性口令验证、电子邮件安全和数据加密等等。

网络和 IT 管理员有责任管理企业用户和安全服务，同时又面临巨大的复杂性。鉴于此种情况，SafeNet 开发了基于微软活动目录架构的令牌管理系统。所有的用户帐号全部在微软的活动目录中创建，eToken 令牌管理系统自动读取这些帐号信息进行管理，同时管理界面完全使用浏览器界面，给管理员带来很大的方便性。eToken 令牌管理系统是一个开放的基于标准的架构，构建于可配置的连接器之上，可以与各种安全应用整合。

3.1.1 eToken TMS 令牌管理系统特点

- ✧ 支持 SafeNet 任何一款 eToken 令牌，包括 eToken Pro, Smart Card, NG-OTP, PASS 和 Flash。能够管理令牌整个生命周期，包括部署和撤销等。
- ✧ 支持多种安全解决方案，包括安全网络访问、PC 和数据保护，以及密码管理
- ✧ 所有的管理员操作以及用户自助管理均通过浏览器界面完成，可以在本地或者远程操作
- ✧ 支持托管服务。在 TMS 中可以设定不同的管理员角色，将这些角色赋予不同管理员以后，这些管理员登录 TMS 就具有了不同的管理员权限。
- ✧ 完整的审计和报表功能，记录所有的管理员操作和用户使用情况。还可以统计出哪些用户正在使用 USB 令牌。
- ✧ 自动地安全备份和恢复用户的密钥和证书
- ✧ 令牌丢失和损坏的处理，特别是当用户在出差的时候丢失令牌的情况下，可以使用 eToken Virtual 实现紧急处理
- ✧ 凭借活动目录技术，完善地支持兼容 LDAP 的用户库，还可以与现有企业用户库完全

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

地集成

✧ 开放的基于标准的连接器架构，通过 TMS Connector SDK 允许企业添加新的安全应用

3.1.2 灵活的支持和实施

TMS，是一个开放的架构，几乎能够灵活的连接到任何一个要求与 token 或智能卡交互的外部服务或系统上 — 标准的或独特的。会创建不同的连接器，以支持 PKI RAs (注册机构)、防火墙或 VPN 应用程序，然后执行用户指定的功能。IT 管理员不需要深入地了解具体的应用程序，TMS 会为他们处理这些细节。

3.1.3 令牌和智能卡的生命周期管理

令牌管理系统提供了强大的工具，能够胜任对令牌的部署和供应以及整个生命周期进行管理。令牌管理系统支持所有的 eToken 设备（包括 eToken Pro USB、eToken Pro 智能卡、eToken NG-OTP 和 eToken Flash），并为管理员提供全方位的令牌管理服务：部署和撤销令牌、通过网页用户可以自己重设密码、自动备份和恢复用户凭证、处理丢失或损坏的令牌等等。

当成功注册了用户令牌，并且将安全应用数据写入到令牌上以后，这些同时会归档到令牌管理系统服务器上。以后万一发生用户令牌丢失或损坏的情况，管理员可以将归档到令牌管理服务器上的数据重新导入到用户新的令牌上，这样原有的数字证书、私钥和各种登录凭证均可以轻松恢复。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

3.1.4 快速简便的用户管理

管理员可以在活动目录的“用户和电脑”视图中，方便地创建用户和用户组，令牌管理系统提供附加的平台能够管理企业用户所关联的令牌、规则、策略和安全应用。通过同一个活动目录的管理界面，管理员可以代替用户执行令牌注册请求，令牌管理系统会自动检查哪个应用程序应该被分配到这个组成员上，要么创建凭证（例如：私钥、数字证书和密码），要么代表用户请求合适的服务，生成的数据都自动加载到令牌上。这样的平台包括安装在企业服务器上后端的应用以及基于 Web 的工具，管理员也可以通过浏览器方便地完成管理工作。令牌管理系统提供提供的 Web 界面可以进行定制，提供企业用户最大的灵活性。

3.1.5 用户自助服务工具

对于那些可以由用户自己完成，不需要管理员介入的操作，例如令牌注册或者密码重设，可以使用用户自助服务来实现，帮助企业节省大量的时间和成本。用户可以快速地处理他们自己的令牌，增强了生产效率同时减轻了 IT 管理员的负担。令牌管理系统提供提供的 Web 界面可以进行定制，提供企业用户最大的灵活性。所有使用 TMS Web 自助服务平台的用户必须在客户端安装 TMS Client 软件。

3.2 eToken 软件开发包(SDK)

eToken 软件开发包应用于强大用户身份验证，PKI 应用程序，导入保护等。

如果您的机构正在自行开发安全防护程序或者其他需要用户身份验证和数码签名的程序，例如电子银行和电子保健软件程序，eToken 软件开发包是最佳的选择。eToken SDK 提供的工具，能将 eToken 安全功能与您的应用程序整合起来。它适用于各种操作系统，并且支持工业标准 API，能与第三方应用程序进行无缝整合。其中有一个接口，可以在在导入之前执行一定的操作，从而可以执行高安全性的系统。eToken 产品套装包括各种设备和产品，都可以同使用 eToken SDK 开发的第三方程序整合。

eToken 软件开发包的优势

- 强大而又灵活的工具，可以把令牌和智能卡与第三方安全应用程序整合。
- 标准的 API，确保与主流的安全应用程序可以互操作。
- 高级的 16 位驱动器使得令牌和智能卡可以集成第三方解决方案，实现计算机的启动

保护。

- 支持多种参数设定

3.3 eToken 认证设备

eToken 的这组设备提供了足够的灵活性，可以满足不同组织机构的需要。从用于 PC 和远程网络的 USB Token，到用于访问控制的智能卡和 ID 证章，eToken 的易用性、高效率和便携性， 使其成为商业机构在现在这个不断变化的数字化时代中保持领先地位的明智选择。所有的设备都支持同样的安全接口，都能与 eToken 和第三方安全程序协同工作。

SafeNet eToken 系列令牌均可以按造客户需求进行定制，包括内置门襟系统芯片、制作 ID 证章、打印或铭刻客户标识等。

3.3.1 多种形式的双因素认证设备

eToken PRO (USB)

eToken PRO 是一个用于数据保护的 USB 令牌。它是一个低成本的、不需要阅读器的智能卡设备，能够启用强大的双要素身份验证，易于部署。eToken PRO 的安全的板载 RSA 1024 位和 2048 位密钥操作，能够安全地存储数字证书、实现安全认证和数字签名所需要的公钥/私钥以及第三方应用程序的静态口令，可以与任何 PKI 或其他的安全架构进行无缝的整合。

eToken NG-OTP

eToken NG-OTP 是一个 USB 和一次性密码混合 token，提供了 eToken PRO USB 的全部功能和 OTP 技术，在分离模式下实现强大的身份验证。eToken NG-OTP 在一个设备里，集成了多种强大的身份验证方法，适用于多种安全相关的解决方案。

eToken NG-FLASH

eToken NG-FLASH 提供了和 eToken PRO 相同的功能，与增加闪存为流动数据存储.

eToken PRO 智能卡

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

eToken PRO 智能卡提供了和 eToken PRO USB 相同的功能，不过使用传统信用卡的外形。标准的智能卡阅读器可以操作 eToken PRO 智能卡。

eToken PASS (一次性密码令牌)

eToken Pass 是一款纯一次性密码令牌。

门禁卡和照片 ID 证章附件

eToken 可以与门禁系统和 ID 证章方案整合。将物理访问和逻辑访问组合在一个设备中。门禁技术与 USB token 和智能卡两种形式都可以整合，取决于企业的需要。eToken 可以非常完美地将对网络的物理访问和逻辑访问，与可以视觉识别的照片证章结合在一起。

3.3.2 SafeNet eToken PRO USB

eToken PRO 为机密应用程序提供了强大的身份验证和有保证的认可机制，例如：电子银行、股票交易、电子商务和商业事务。

eToken PRO 的板载 RSA 1024 位和 2048 位密钥操作非常安全，能够与公钥基础设施无缝整合。eToken PRO 可以生成并且存储用户的个人证书，例如私钥和数字证书，存储在受保护的智能卡芯片里。用户的私钥永远不离开 eToken。

eToken PRO 物有所值、易于使用，是一款不需要阅读器的智能卡设备。可以把它放在钥匙环上或者口袋里，从一个工作站带到另一个工作站。

利用高级的智能卡技术，eToken PRO 提供了双要素和双向的身份验证技术。eToken 板载了先进的加密处理器，通过了 ITSEC LE4 安全认证，使用物理防盗和防水包装，是实现企业的网络和电子商务安全的理想选择。

eToken PRO 的特色和优势：

- 板载生成公钥和私钥，私钥永远不会离开 eToken。
- 不需要再开发或整合：eToken 支持标准的安全接口和多种安全客户端程序。
- 灵活的开发工具，实现与第三方应用程序的无缝整合。
- 便携的 USB 设计,不需要特定的阅读器。
- 双因素身份验证,既需要 eToken 本身，还需要 eToken 密码。
- 安全地存储用户数字证书、密钥和机密信息。
- 可以选择标签和颜色，方便品牌推广。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

适用的安全服务和应用：

- 安全的远程接入（VPN/Web）。
- 安全的外联网/内联网访问。
- 安全的网络登录。
- 安全的在线 B2B 和 B2C 服务：金融、教育、医疗、商务等等。
- 对电子商务的交易进行签名。
- 受保护的邮件通信：加密和签名。
- PC 安全保护：启动保护和文件加密。

eToken PRO 规格指标

支持操作系统	Windows 2000/XP/2003/Vista; Mac OS X; Linux
API 及所支持的标准	PKCS#11 v2.01, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
型号	32K: Siemens CardOS / 32K memory 64K: Siemens CardOS / 64K memory Java: Java Virtual Machine / 72K memory
板载安全算法	RSA 1024-bit / 2048-bit, DES, 3DES, SHA1, SHA256
安全认证	FIPS 140-1 L2&3; 通用标准 EAL4+/EAL5+ (智能卡芯片及操作系统) 申请中: FIPS 140-2 and CC EAL4+ PP-SSCD (不同型号的安全认证不同，请质询)
尺寸	52 x 16 x 8 mm (2.05 x 0.63 x 0.31 inches)
所支持的 ISO 规范	支持 ISO 7816-1 至 4”规范
运行温度	0 C to 70 C (32 F to 158 F)
存储温度	-40 C to 85 C (-40 F to 185 F)
湿度等级	常态下 0-100%
防水认证	IP X8 – IEC 529
连接器	USB type A (Universal Serial Bus)
封装	坚固的塑膜封装，显窃启
数据保存期限	不少于 10 年
存储器重写次数	不少于 50 万次

3.3.3 SafeNet eToken NG-OTP

SafeNet eToken NG-OTP 是一款混合 USB 和一次性密码的令牌。具有基于智能卡的 eToken PRO 的 PKI 加密、签名功能和安全的凭证存储功能，以及使用一次性密码技术验证网络访问用户身份的功能。eToken NG-OTP 高的灵活和通用，同一个设备支持各种不同的强身份验证方式以及相关的安全解决方案。eToken NG-OTP 是满足企业不同安全环境下的最终的解决方案，支持大量的网络、应用和客户需求。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

混合设备的优势

eToken NG-OTP 将多种验证方式集成到单个安全设备上。例如，员工使用强身份验证来访问公司网络，在办公室里将 eToken 插入到计算机的 USB 端口上。在有些场合无法连接 USB，例如在网吧里，用户可以使用相同的令牌，通过 eToken 的一次性密码身份验证建立 VPN 连接安全地访问网络。这样，能够使用 eToken 在大量不同的场合进行双因素身份验证。

eToken NG-OTP 的特色

- 带有一次性密码验证功能的 USB 令牌（拥有 LCD 显示屏、电池和一次性密码产生按钮）
- 低电池指示标志提醒用户更换电池
- 智能卡支持 RSA 1024 位和 2048 位密钥长度，3DES 算法和 SHA1 算法
- 支持 OATH 一次性密码协议
- 标准的 PKI 支持 CAPI、PKCS11 和 RADIUS OTP
- 完全兼容 eToken PRO
- 使用智能卡芯片高度安全地实现 PKI 和一次性密码运算
- 健壮的即插即用 USB 连接
- 支持模块化的一次性密码算法
- 强双因素身份验证：要求令牌本身以及对应的密码
- 使用高级的芯片内数字签名技术实现不可否认性
- 通过植入 eToken 设备内的门襟系统线圈可以集成安全的逻辑和物理访问

eToken NG-OTP 好处

- 灵活和通用的解决方案：PKI、一次性密码和安全的凭证存储
- 高度安全的智能卡技术
- 零脚印认证，一次性密码认证验证不需要安装客户端软件
- 轻松便捷的后端服务器配置
- 改进的低成本密码管理解决方案
- 长生命周期

eToken 实现安全的服务和解决方案

- 安全的网络访问
- Windows 和基于 Web 应用程序验证
- 电子邮件加密和数字签名
- 在线金融服务、网上银行和电子商务应用的强身份验证和安全的交易签名
- VPN 身份验证
- 远程访问服务器（RAS）身份验证
- 个人电脑安全：启动保护、磁盘加密和文档加密
- 在线政务服务：市民信息、设备登记、退税和医疗服务
- 安全的门襟访问

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

eToken NG-OTP 规格指标

支持操作系统	Windows 98/98SE/Me/2000/XP/NT4.0 SP6 and later/Vista; Mac OS X; Linux
API 及所支持的标准	PKCS#11 v2.01, CAPI (Microsoft Crypto API), Siemens/Infineon APDU commands, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
智能卡内存	32K, 64K, 72K
板载安全算法	RSA 1024-bit / 2048-bit*, DES, 3DES (Triple DES), SHA1 (*) Available with 64K model
安全认证	通用标准 EAL5/EAL5+ (智能卡芯片) / EAL4+ PP-SSCD (智能卡芯片操作系统) FIPS 140-2 and CC EAL4+ PP-SSCD 申请中
OTP 安全算法	遵循 OATH（基于 HMAC-SHA1）
所支持的 ISO 规范	支持 ISO 7816-1 至 4”规范
封装	坚固的塑膜封装，显窗启
电池寿命	生成 10000 次一次性密码/5 年, 可更换电池
数据保存期限	不少于 10 年
存储器重写次数	不少于 50 万次

3.3.4 SafeNet eToken PRO 智能卡

eToken PRO 智能卡使用标准智能卡阅读器操作。

eToken PRO 智能卡为机密应用程序提供了强大的身份验证和有保证的认可机制，例如：电子银行、股票交易、电子商务和商业事务。

eToken PRO 智能卡的板载 RSA 1024 位和 2048 位密钥操作非常安全，能够与公共密钥底层架构无缝整合。eToken PRO 可以生成并且存储用户的个人证件，例如私人密钥、密码和数码认证书，存储在受保护的智能卡芯片里。用户的私人密钥永远都在 token 里。

利用高级的密语智能卡技术，eToken PRO 提供了双要素和双向身份验证认证。eToken 板载了先进的加密处理器，通过了 ITSEC LE4 安全认证，使用物理防盗和防水包装，是实现企业的网络和电子商务安全的理想选择。

特点

- 使用标准的智能卡阅读器操作
- 支持公钥基础设施(PKI)，板载 1024 位和 2048 位 PKI 密 钥生成机制。
- 板载 RSA 1024 位和 2048 位 身份验证和数字签名。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

- ITSEC LE4 认证的，高度安全的逻辑和物理智能卡保护。
- 能够连接 Crypto API 和 PKCS #11。
- 安全存储和强健的文件系统。
- 与主流的 PKI 和安全客户端能够即插即用地连接。

优势

- 使用高级 PKI 数字签名技术，完全认可：数据记录在 eToken 内部的智能卡芯片上，远离了危险的电脑环境。
- 板载 PKI 生成：私人密钥不会泄露。
- 不需要再开发或整合：eToken 企业版支持标准的安全接口和多种安全客户端程序。
- 灵活的开发工具，实现与第三方应用程序的无缝整合。
- 双要素身份验证：既需要 eToken 本身，还需要 eToken 密码。
- 安全地存储用户授权书、密钥和机密信息。
- 可以选择标签和颜色，方便品牌推广。

支持的安全服务和应用程序

- 网上商业服务：为电子银行和股票交易程序提供身份验证和交易签字。
- 外网/内网访问。
- 网上政务：居民信息、车辆注册、返税和医疗保健。
- 电子商务 B2B 和 B2C 服务：电子商务程序的身份验证和事务签字。
- 虚拟专网（VPN）方案：双要素身份验证。
- 远程访问服务器 (RAS) 身份验证。
- 受保护的网络登录。
- 受保护的邮件通信：加密和签字。
- PC 安全保护：启动保护和文件加密。
- ID 卡。

eToken PRO 智能卡规格指标

支持操作系统	Windows 2000/XP/2003/Vista Mac OS X; Linux (32K and 64K token models only)
API 及所支持的标准	PKCS#11 v2.01, Microsoft CAPI, PC/SC, X.509 v3 certificate storage, SSL v3, IPSec/IKE
型号	32K: Siemens CardOS / 32K memory 64K: Siemens CardOS / 64K memory Java: Java Virtual Machine / 72K memory
板载安全算法	RSA 1024-bit / 2048-bit, DES, 3DES, SHA1, SHA256
安全认证	通用标准 EAL4+/EAL5+ (智能卡芯片及操作系统) 申请中: CC EAL4+ PP-SSCD (不同型号的安全认证不同，请质询)
所支持的 ISO 规范	支持 ISO 7816-1 至 4”规范
数据保存期限	不少于 10 年
存储器重写次数	不少于 50 万次

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

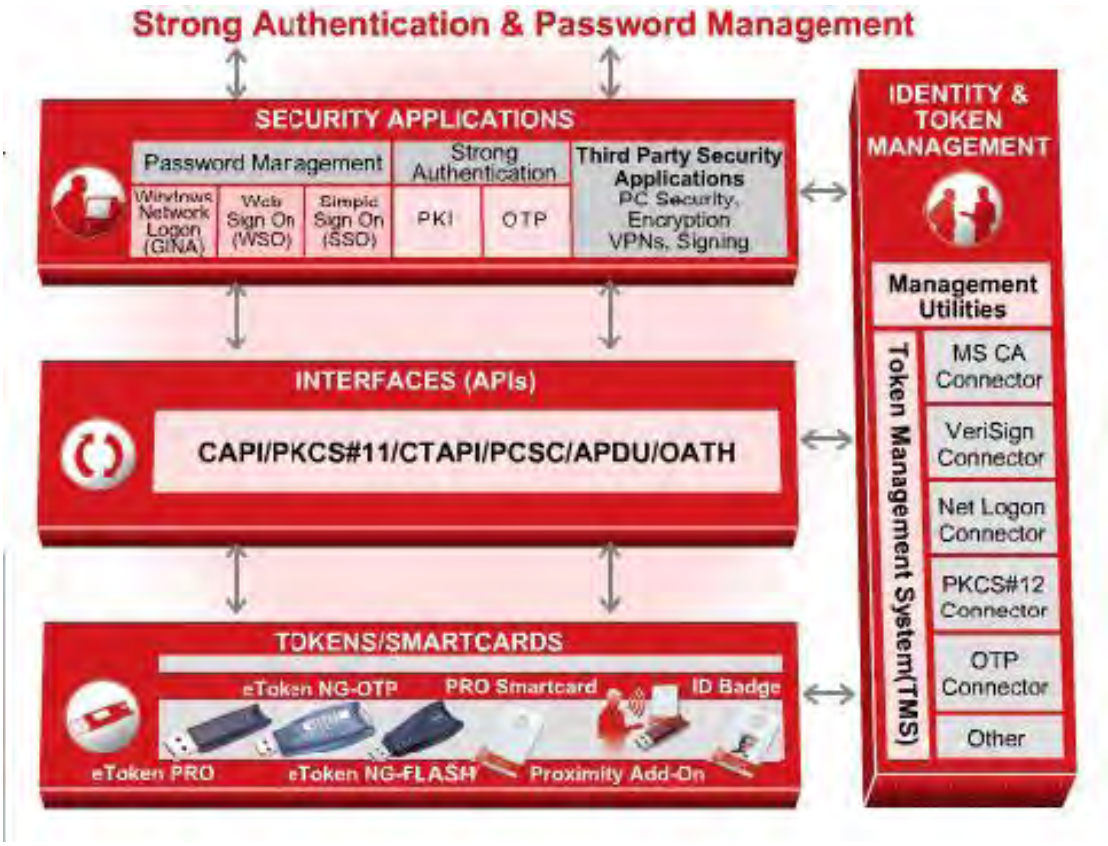
4 SafeNet eToken 解决方案

在商业全球化的今天，您需要一个解决方案，保障您无论何时何地都可以安全地访问商业信息。但它可能需要大量的资金投入。而 eToken 正为此提供一个应用广阔地标准平台，可以降低资金投入和管理成本。

SafeNet eToken 提供了强大的身份验证和密码管理解决方案，具体包括：

- ✧ 增强安全保护，确保信息访问的安全性
- ✧ 高效的密码管理
- ✧ 不管去哪里，都可以随身携带您的个人证书

eToken 产品提供了健壮而又灵活的框架，能够与现在顶尖的安全解决方案整合，是能够满足您对于身份验证和密码管理的需要的解决方案。

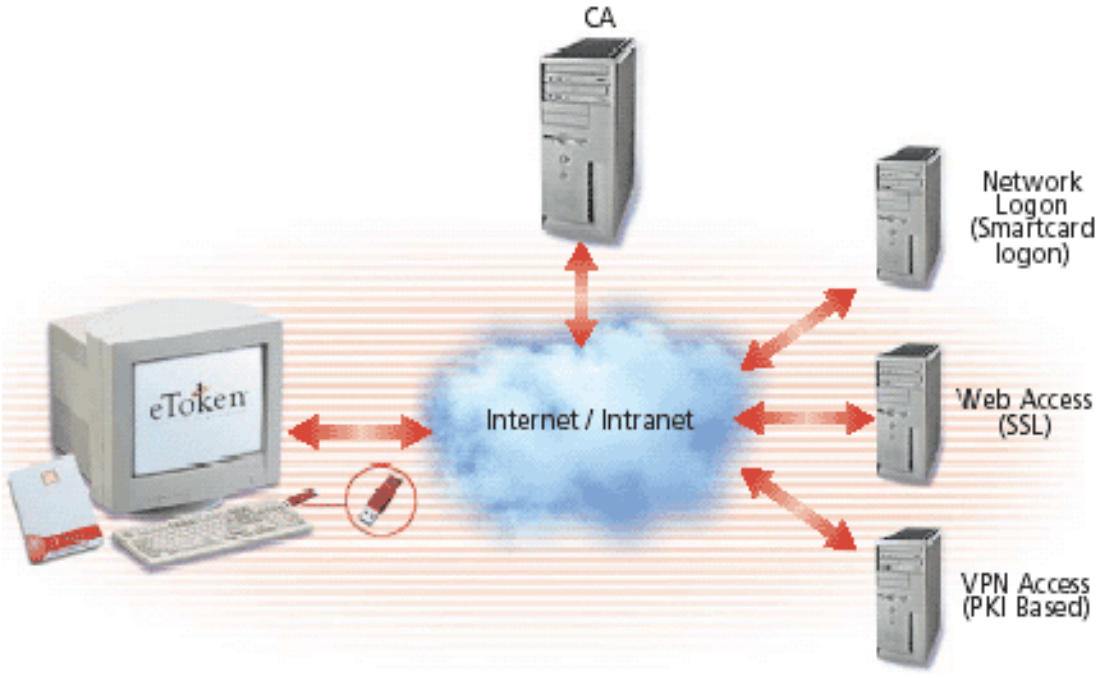


地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

4.1 eToken PKI 智能卡方案

eToken PKI 解决方案，能让 PKI 软件在基于 USB 的 eToken 或 eToken 智能卡内生成、存储和操作私人密钥和数字认证，创造了一个操作简便、易于携带的安全环境。eToken PKI 方案含有与工业产品整合所需要的所有 PKI 组件和驱动程序。用户不再需要为不同的帐号设置不同的密码，仅仅需要 eToken 密码。所有的验证数据都安全方便地存储在 eToken 上，可以在任何一台配置好的计算机上使用。

公钥基础设施（PKI）可用于多种安全服务，包括用户身份验证和事务认可。SafeNet 的 eToken PKI 解决方案为企业机构带来了强大的双要素用户身份验证，适用于网页访问，远程 VPN 访问，网络登录，PC 保护，电子邮件保护和任何标准的 PKI 软件。



SafeNet eToken PKI 解决方案的特色：

- 支持所有的 PKCS#11 PKI 软件
- 通过 CAPI 支持所有的微软安全应用程序和服务
- 支持标准的用户存储器，例如：标准 X.509v3 认证格式的 AD 和 LDAP
- DES, 3xDES, DES-X, MD5, RC2, 4, 5, 支持高达 2048 位的 RSA 密钥
- Win9x, ME, NT, 2000, XP
- Netscape 和 Internet Explorer 网页浏览器
- 支持标准的 CA 系统：Microsoft, Netscape, Entrust, Baltimore, VeriSign

SafeNet eToken PKI 解决方案的优势：

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

- ✧ 对用户私人证书和数字认证进行高级别的安全保护。用户可以完全放心地对电子交易进行验证、加密、签字和解密。
- ✧ 启用双因素验证，电子商务和电子银行软件可以通过硬件设备确保高级别的安全性。
- ✧ 在 eToken 上安全地生成、存储用户的密钥和认证，能与任何标准 PKI 软件一起透明式协作。

4.1.1 eToken 加强 Windows 的网络登录

微软 Windows 操作系统提供了整合的网络登录解决方案，登录 Windows 域计算机时的身份验证机制覆盖了从简单的用户名和密码到全面的 PKI 智能卡验证的范围。eToken 使得网络管理员对基于密码的登录和智能卡登录，都可以执行强大的双因素用户身份验证机制。

在微软 Windows 网络登录(GINA)机制中，缺省提供了使用智能卡中的数字证书登录域环境的功能，所以配置和实施起来非常稳定和可靠。由于微软的域结构非常复杂，包含了许多通讯协议和组件，所以如果自己开发一套域登录解决方案的话，在兼容性上存在很多问题。而使用 Windows 自带的智能卡登录功能，不会有任何兼容性的问题，同时也不需要改变 Windows 的登录界面，给用户一个熟悉的操作环境。

解决方案优点

- ➢ 针对智能卡登录方案，eToken 提供了安全的板载生成 PKI 密钥和数字证书的机制，由于私钥永远不会离开 eToken，同时用户资料安全地存储在 eToken 设备中，增强了安全性和可移植性。
- ➢ 通过双因素身份验证机制，要求用户必须提供 eToken 设备和 eToken 密码才能使用此设备。eToken 提供了强大的保护能力，以及紧凑的 USB 设备带来的便携性，保护您的企业网络，避免未经授权的访问。
- ➢ 支持两种模式：一个 eToken 既可以支持基于密码的身份验证，在 eToken 中保存 Windows 操作系统的登录帐号和密码；也可以支持基于 PKI 的网络身份验证，在 eToken 中安全地保存用户的网络访问数字证书，确保最大的灵活性和易用性。
- ➢ 支持在一个 eToken 上存储和管理多个用户资料和第三方应用登录凭证，可以配合 SafeNet eToken SSO 软件，无缝地升级到单点登录解决方案。

系统安装和实施步骤

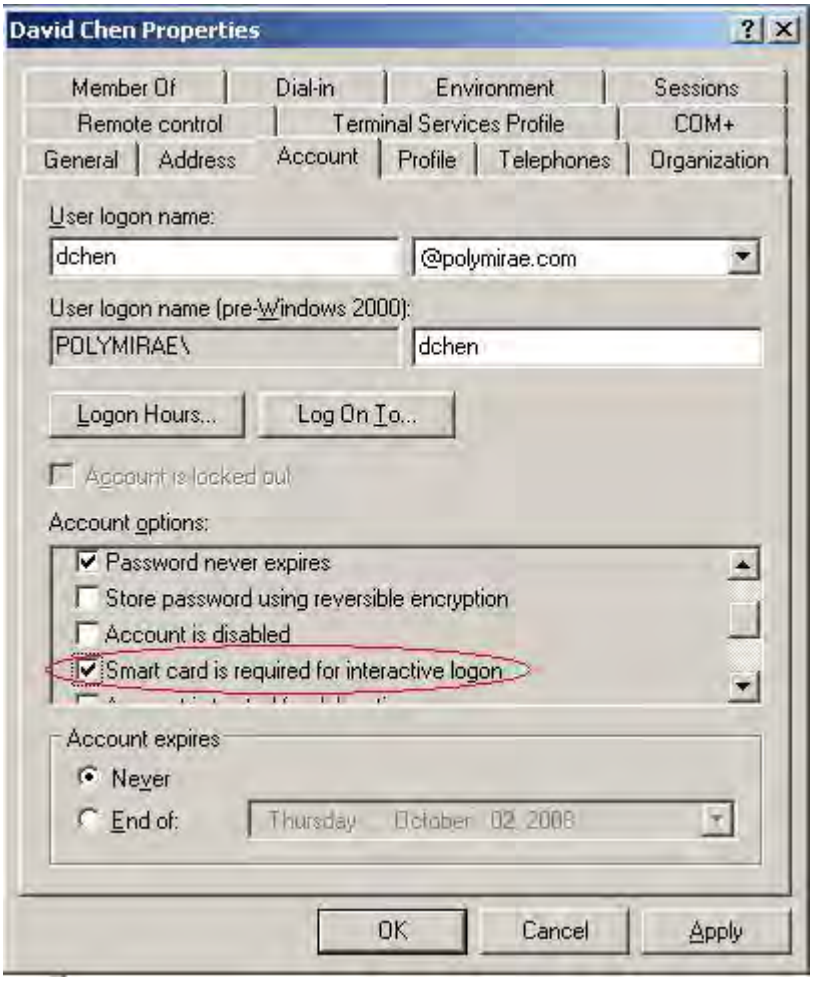
- ➢ 在现有域成员服务器上或者新建的域服务器商安装 IIS 以及 SafeNet 令牌管理系统。
- ➢ 安装 Windows 操作系统中自带的 Microsoft Enterprise CA，配置证书模板，允许用户申请 Windows 智能卡登录证书。
- ➢ 配置 SafeNet 令牌管理系统，允许管理员在分配令牌的同时，系统会自动到 MSCA 上申请证书并且自动写入到用户的 eToken 中。
- ➢ 在 AD 中创建用户并且分配 eToken，用户的 Windows 登录证书自动写入到 eToken

中，将 eToken 发放给用户。

- 在用户客户端电脑上需要安装 PKI Client 软件才能够正常读取 eToken 中证书。
- 用户拿到令牌以后，启动计算机，如果安装了 PKI Client 以后，在启动界面上会显示下图所示的智能卡图标。

- 在开机界面中插入 eToken，显示输入 PIN 码界面。

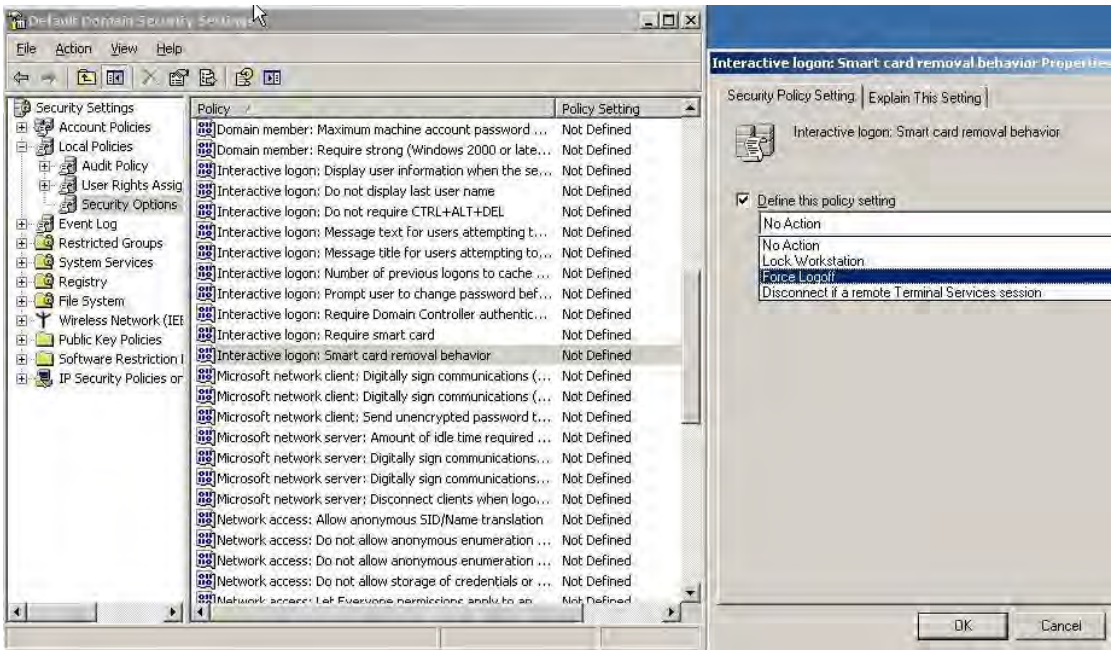
- 输入正确的 eToken 密码以后，就可以安全地登录操作系统。
- 管理员可以定义此用户必须使用智能卡才能够登录操作系统，即使知道了操作系统的用户名和密码也无法登录操作系统，增强了系统的安全性。



- 当用户试图使用静态密码登录操作系统时，显示出错信息。

- 管理员还可以根据用户组策略配置当用户拔出 eToken 时候计算机的响应，管理员可以有几个选项可以选择：没有操作；锁定计算机；强制退出和中断远程终端连接会话。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103



4.1.2 VPN 技术安全（安全远程访问）

eToken 可以和主流的 VPN 系统无缝整合，为远程访问企业网络提供强大的用户身份认证。

SafeNet eToken 支持业界顶尖的 VPN 系统，包括：Cisco Systems、Check Point 和 Microsoft 等任何支持数字证书认证的 VPN 系统。

用户把 eToken 插入计算机，然后启动 VPN 客户端程序并且选择存储在 eToken 中的数字证书，在认证过程中需要输入正确的 eToken 密码，当数字证书有效并且通过 VPN 网关的认证以后，就可以建立安全加密的数据通道。而一旦用户拔出 eToken，VPN 通道会自动中断，确保了系统的安全性。如果使用一次性密码（OTP）技术实现 VPN 认证的话，则无法实现自动中断的功能。

通过使用 eToken 加数字证书登录 VPN 的解决方案，用户可以获得安全、可靠、双要素身份验证。

4.1.3 Web 登录

eToken 为访问受保护的 Web 资源与敏感信息传输提供强大的用户身份认证。当用户启动浏览器访问应用服务器网站时，可以在浏览器和服务器之间建立安全加密的 SSL 通道，

同时要求用户出示有效的数字证书，只有验证了数字证书有效性以后，用户才能获得应用程序的访问权限，确保了只有合法的用户才能访问关键的企业应用。

4.1.4 PC 和笔记本的安全防护

eToken 能够与多种数据保护系统无缝整合以保护用户的计算机，保护范围覆盖：完全的磁盘加密、启动保护、加密特定的文件和文件夹。

笔记本和 PC 的安全影响整个组织的安全

如今，丢失或被盗一台笔记本可能就意味着整个机构的安全性受到威胁……管理机构作出严厉的罚款或其他处罚……一旦被公开，还有其他的恶性后果和损失，有时法律要求必须公开。

如何保护你的机构，确保数据安全？

用于启动保护和文件/文件夹的基于软件的解决方案是个好的开始，但是它仍然依靠密码。而且，密码很容易被猜测、写下、被盗、共享、破解，是安全方面最薄弱的环节。

结合启动保护和数据加密方案，eToken 用户可以得到：

- 增强的笔记本加密和 PC 安全保护
- 板载加密机制
- 标准的通用串行总线
- 非常便携
- 物有所值的身份验证
- 集中管理

PC 安全方案合作伙伴

SafeNet eToken 与全球范围内的业界领先的 PC 保护软件提供商合作，把 eToken 基于 USB 的双要素验证方案整合到他们的产品中：

- 启动保护
- 磁盘加密
- 文件/文件夹加密

4.1.5 电子邮件的安全防护

eToken 通过标准化接口，与主流邮件客户端无缝整合，对邮件进行加密和签名。支持的 SMIME 电子邮件程序包括微软的 Outlook、Outlook Express 和 Netscape 公司的

Messenger。

4.1.6 数字签名（不可否认性）

eToken 使用 PKI 技术对文档、交易数字签名，保证电子交易的真实性。

4.2 eToken 一次性密码（OTP）身份验证解决方案

SafeNet eToken 为企业提供了物有所值的强大而又灵活的用户身份验证方案。eToken OTP 方案，实现了无需客户端的登录方式，使用了一次性密码身份验证技术，结合 eToken 智能卡解决方案，为您的数字商务资源提供了强大而又灵活的安全保护。

商业组织努力地通过扩展 IT 基础设施建设来提高自身的商务处理能力。相应的，强大的身份验证解决方案成为保障 IT 安全的关键因素。企业通过保护对企业网络和商业数据的访问， 使得消费者、合作伙伴和雇员可以随时随地（在办公室、家里或路上）地使用商务软件。

在基于智能卡的身份验证、密码管理和公钥基础设施（PKI）方案等领域内，SafeNet 都取得了稳固的领先地位，现在提供基于一次性密码技术的身份验证解决方案。

eToken OTP 方案满足您对身份验证的需求，增强您的电子商务能力。
eToken OTP 方案基于 eToken NG-OTP 设备，是 SafeNet 独创的基于智能卡的混合 token。可以在连通模式（采用 USB 连接）或分离模式（采用 one-time 密码）下安全地访问您的网络和应用程序。

eToken OTP 解决方案由用于后台验证的 eToken RADIUS 服务器和整合的 RADIUS 软件组成，包括：领先的 VPN 方案、网页访问方案等。OTP 解决方案由 SafeNet 的令牌管理系统提供完善的支持和管理，能够应对整个企业的令牌部署和生命周期管理。

优势

- ✧ 提供灵活的用户身份验证基础设施，满足您的需要
- ✧ 客户端不需要安装额外的软件来支持一次性口令认证
- ✧ 只需极少的 IT 帮助和维护
- ✧ 与 eToken 智能卡身份验证和安全服务完全整合

eToken NG-OTP：USB 和 OTP 混合 Token

SafeNet eToken NG-OTP 是一种混合的一次性密码 USB token，它把基于智能卡的 eToken PRO 的全部功能与 OTP 技术集成在一起，为用户提供了分离模式下的高强度用户身份验证。

SafeNet eToken 一次性密码身份验证解决方案的特性：

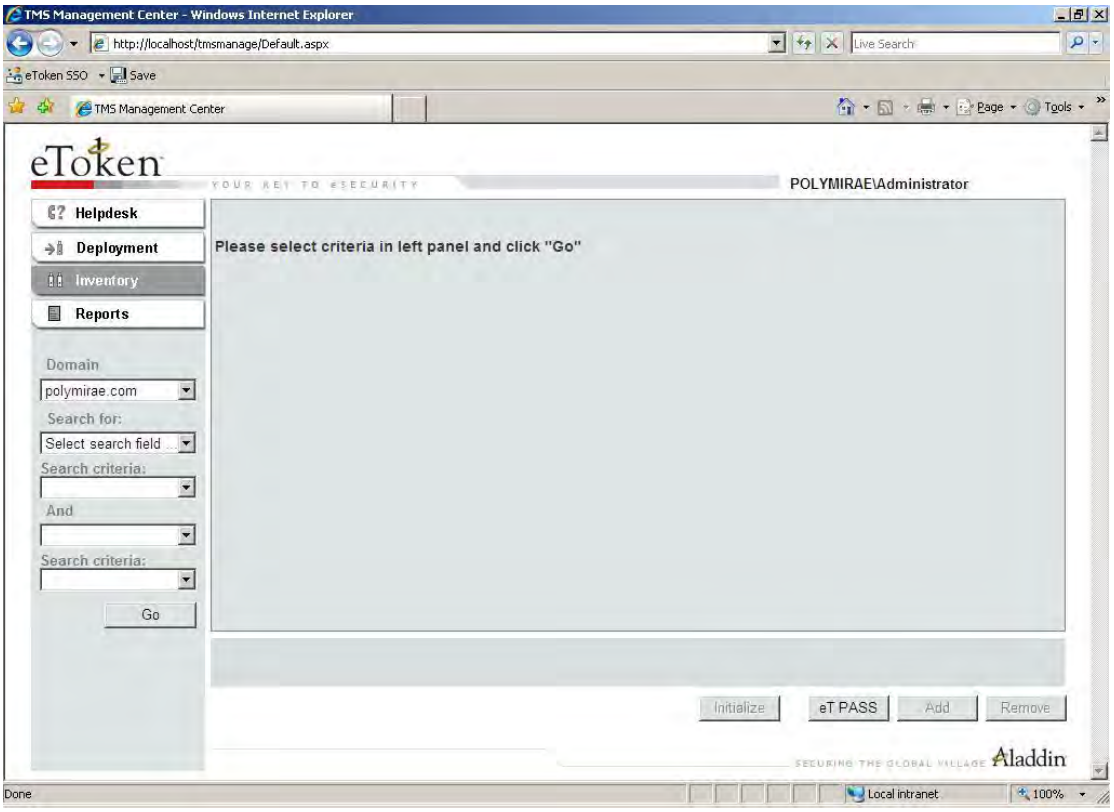
- ➢ 基于 eToken RADIUS 服务器的 OTP 身份验证
- ➢ 与 SafeNet Token 管理系统全面整合，提供了完善的 token 供应和生命周期管理
- ➢ 能够安全的访问商业组织的网络和商业程序
- ➢ 强大的双要素身份验证
- ➢ 不留痕迹 - 无需安装客户端
- ➢ 支持所有兼容 RADIUS 的解决方案
- ➢ 支持 eToken 智能卡解决方案，包括加密电子邮件、安全网页访问、安全 VPN 访问等等。

4.2.1 简单管理和自助服务

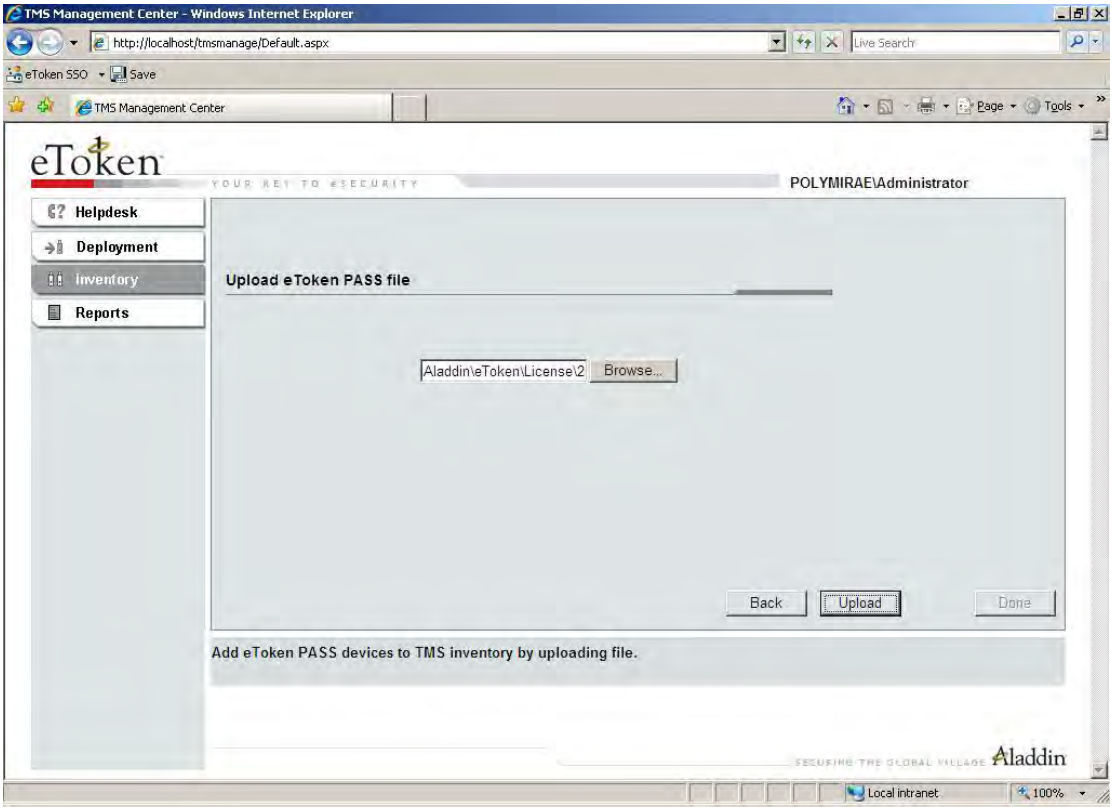
以下是使用 TMS 进行令牌管理和用户自助服务的操作示意图。

1. 打开浏览器，访问 http://localhost/tmsmanage，选择~~I~~nventory”--> ~~e~~T PASS”，

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

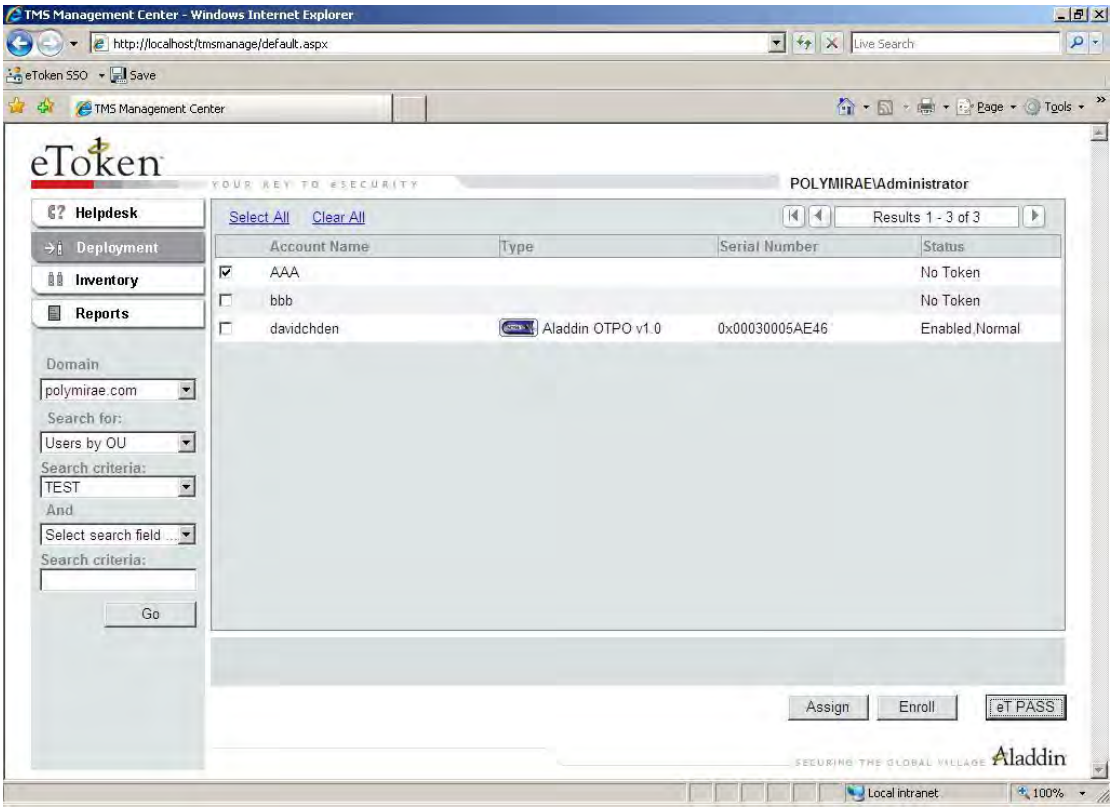


2. 选择种子文件，导入令牌种子。



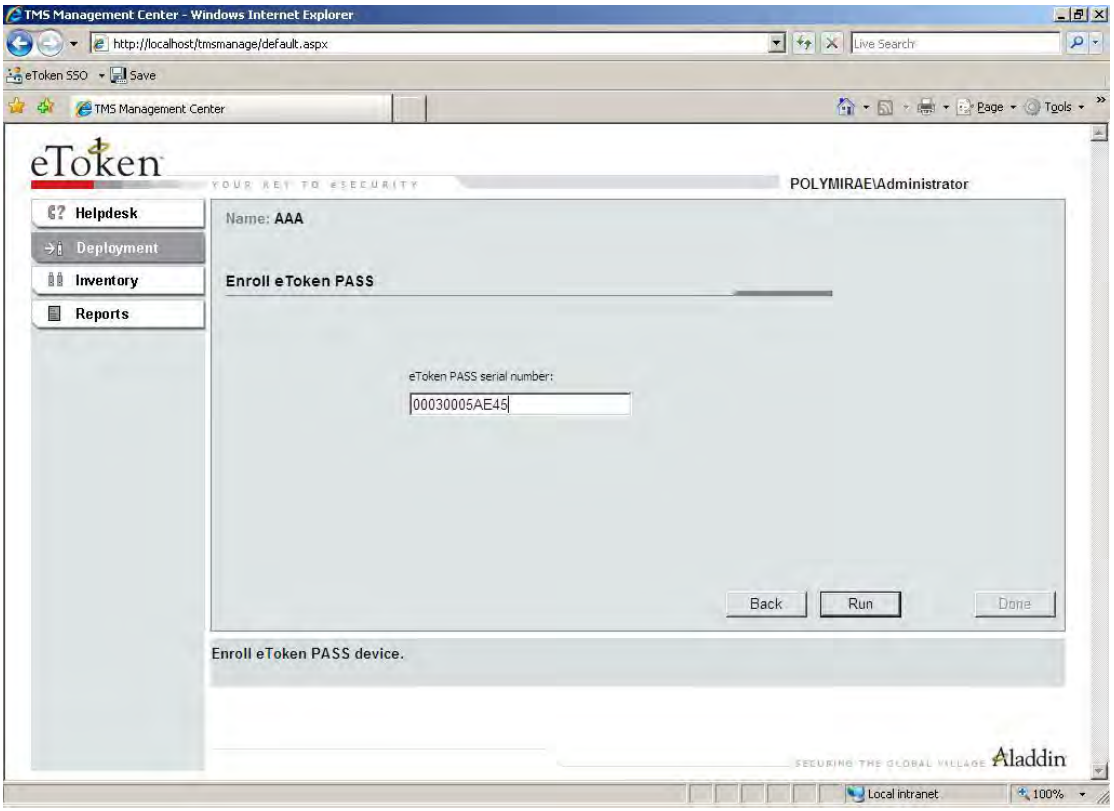
地址：上海市徐汇区桂林路 396 号 3 号楼 611 室　(200233)
电话：8621-64701090　　传真：8621-54640133-803
E-mail：jackwrw@msn.com　　网址：http://www.wang-cai.com
免费电话：400-600-9103

3. 选择“Deployment” → Search for “Users by OU”→ Search criteria 为测试 OU 名称例如“TEST”，选择 GO，然后选择需要分配令牌的用户点击 eTPASS

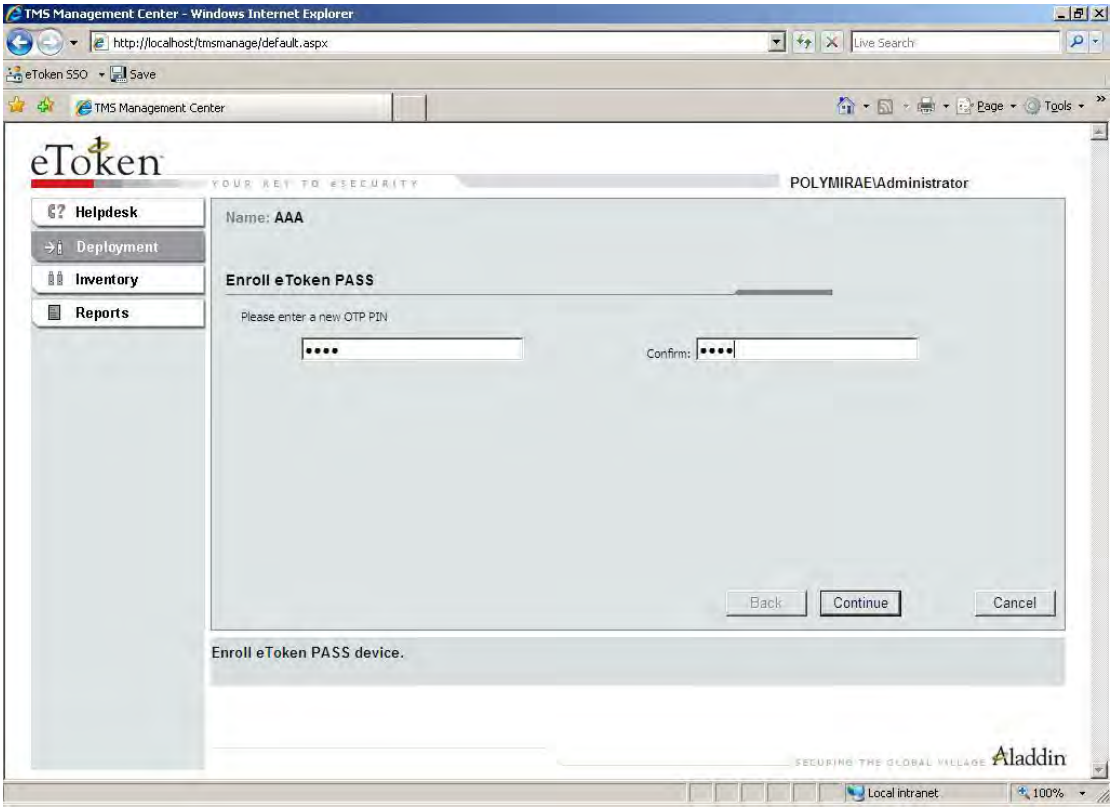


4. 输入令牌背面的序列号，点击 Run 继续

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

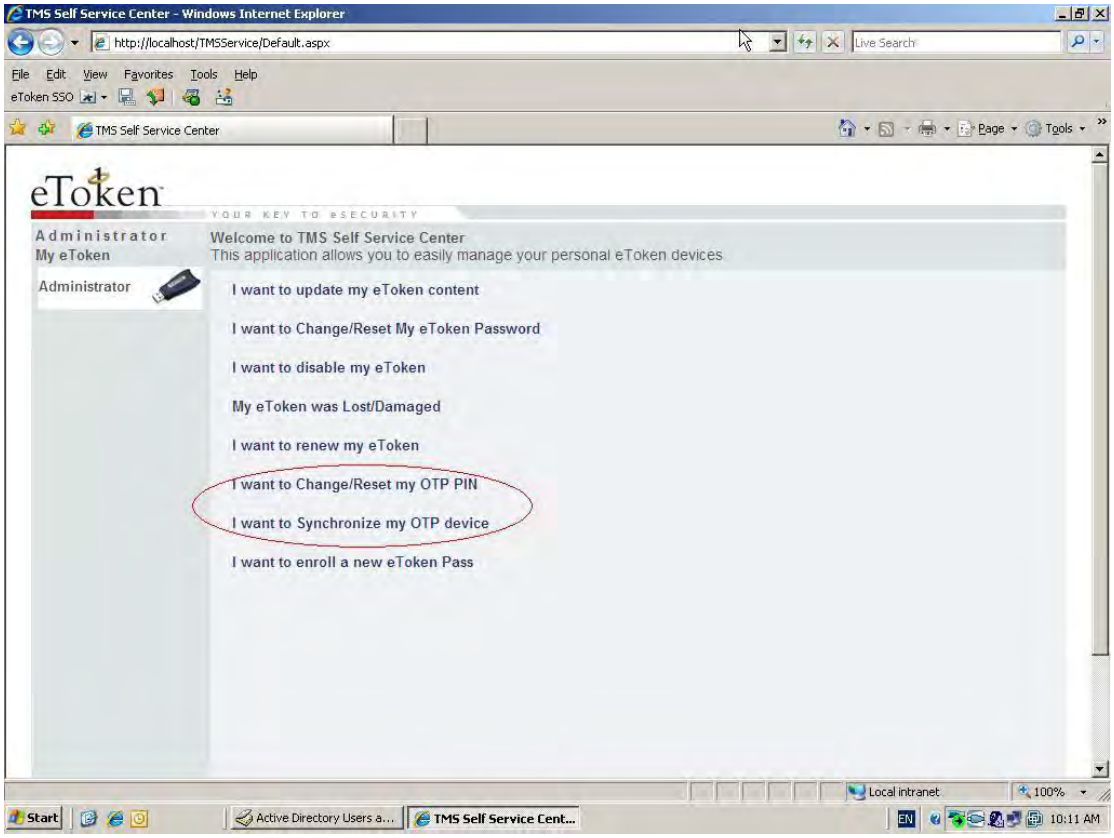


5. 设定初始 OTP PIN 码，点击 Continue 完成令牌分配



地址：上海市徐汇区桂林路 396 号 3 号楼 611 室　(200233)
电话：8621-64701090　　传真：8621-54640133-803
E-mail：jackwrw@msn.com　　网址：http://www.wang-cai.com
免费电话：400-600-9103

6. 最终用户可以访问 TMS 自助平台来更改 PIN 码或者同步令牌



4.2.2 eToken 与 Citrix 集成

Citrix WI 是一个应用部署系统，允许用户通过标准的 Web 浏览器来访问 MetaFrame Presentation Server。

Citrix WI 为用户动态地创建 MetaFrame 服务器集群的 HTML 表现，为每个用户展现有权访问的所有发布在 MetaFrame 服务器集群上的应用程序。

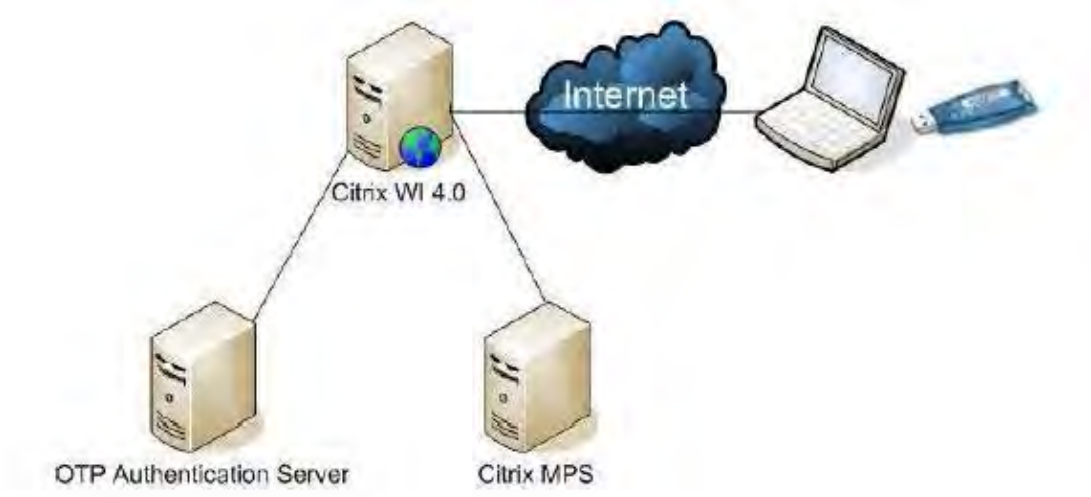
eToken OTP Authentication 2.0 for Citrix WI 是专门为 Citrix WI（Web Interface）4.0 开发的身份验证解决方案，通过要求使用一次性密码技术确保高级别的安全来防止 WI 未授权的访问。

多个 OTP 身份验证服务器以及多个域可以配置成使用此解决方案要求 OTP 身份验证。

OTP 身份验证使用场景

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

在此场景中，一个远程用户启动 Web 浏览器。 Citrix WI 4.0 到 OTP 身份验证服务器和活动目录上验证用户的登录凭证，然后重定向用户至 WI 应用程序。



在 Citrix WI 4.0 和 OTP 身份验证服务器组件之间触发以下过程来建立一个安全的连接：

- 远程用户启动 Web 浏览器来连接 WI 4.0
- WI 4.0 显示登录页面来采集用户的登录凭证
- 用户提供以下登录凭证来实现身份验证：包括密码在内的域网络登录凭证；eToken NG-OTP 或者 eToken PASS 上产生的 OTP 代码发送至 OTP 身份验证服务器
- 一旦通过 OTP 身份验证，WI 4.0 将用户的域网络密码送至活动目录进行身份验证
- 如果两次身份验证均通过，用户被转至 WI 应用主页面

最小要求

安装 eToken OTP Authentication 2.0 for Citrix WI 的预先要求是：

- Web Interface for Presentation Server 4.0
- eToken OTP Authentication Solution 2.0
- SafeNet TMS 2.0
- eToken NG-OTP 或者 eToken PASS

OTP 登录 Citrix WI 4.0

eToken OTP Authentication 2.0 for Citrix WI 安装添加一个 PASSCODE 字段到 Citrix WI 登录页面。

以下是登录到 Citrix WI 4.0 的过程：

- 使用客户端 Web 浏览器访问 Citrix WI 4.0 登录页面，显示以下登录界面

- 按照要求输入用户名、密码和域名。根据 eToken OTP 身份验证解决方案的配置，在 PASSCODE 字段输入合适的值：单独 OTP 代码或者 OTP PIN + OTP 代码。

4.2.3 网络设备保护

在现有的网络配置中，用户可能通过拨号接入公司网络；同时也可能有大量的路由器连接到互联网，即使在企业内部也有大量的交换机，由于若口令带来的安全隐患，管理员可能需要定期修改路由器和交换机上的管理员密码，这种方法并没有从根本上堵住安全隐患，同时也带来大量的管理负担。所以需要考虑使用双因素强认证，确保只有合法用户才可以访问网络资源。

主流的网络设备（包括路由器和交换机）均支持 Radius 协议来集成第三方认证服务器，缺省情况下是在这些设备上创建帐号并且设置静态密码，管理员通过这些静态密码登录网络设备。如果需要切换到令牌认证的话，需要在这些网络设备中启动 Radius 认证，指定 SafeNet etoken 一次性密码认证模块所在的认证服务器的 IP 地址，在认证服务器和网络设备上设置相同的加密密钥来加密数据通讯。当用户需要访问这些网络设备时，提示输入用户名和双因素认证吗，用户输入认证信息以后，网络设备将这些认证信息通过 RADIUS 协议传送到 SafeNet 认证服务器进行用户认证，最后将认证结果返回给网络设备，只有那些通过认证的用户才能够访问这些网络设备，确保了管理员身份的安全性。

目前为止，微软的拨号服务器、思科、3COM 和华为等这些主流的网络设备均可以支持 SafeNet eToken 认证。如果需要在思科的网络设备上启动 AAA 认证，使用 SafeNet eToken 认证管理员的登录的话，只需要加上以下几行配置即可，非常简单：

aaa new-model
aaa authentication login default radius line enable
radius-server host xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646
radius-server key –your key”

如果顾虑到 SafeNet eToken 认证服务器发生故障导致管理员因为无法进行认证从而无法登录网络设备的话，可以配置网络设备首先使用 Radius 进行认证，如果无法联系到 SafeNet 认证服务器，可以使用本地配置的 Line 或者 Enable 的静态密码进行。

4.2.4 防火墙和 VPN 保护

在当今竞争越来越激烈的商业环境中，如何以最快的速度，安全可靠地获得信息变得越来越重要，同时由于互联网的应用越来越普遍，使用 VPN 实现远程接入的方式也越来越广泛。举例来说，许多企业每天都会有大量员工出差，这些员工需要安全接入公司内部网络访问电子邮件和其他重要的价格和公司信息；另外，许多企业正在建设或者即将建设办公自动化系统，企业员工可以在远程办事处甚至家里就可以象在公司内部网络那样登录 OA 系统处理每天事务；对于制造性企业来说，改进与合作伙伴和代理商的关系非常重要，必须让他们通过 Extranet 很快了解公司营销策略，访问瞬息万变的价格，并通过 Extranet 快速下单。所有这些需求都遇到了同样棘手的问题，如何确保从互联网接入公司内部网络的人员的身份呢？VPN 可以通过加密实现 VPN 客户端与 VPN 网关之间的数据通讯的机密性，但是只有与动态令牌一起使用才能真正确保企业网络的安全性。

市场上主流的 VPN 厂商已经集成了 RADIUS 认证协议在 VPN 设备中，管理员只需要在图形界面上非常简单地配置 RADIUS 信息就可以实现双因素认证功能。而客户端只需要安装 VPN 客户端程序，不需要安装额外的软件来支持双因素认证。当用户需要通过防火墙或者 VPN 网关接入企业内部网络时，只需要在原来输入用户名/口令的地方输入双因素认证码，然后由这些网络设备内置地代理软件或者标准的 RADIUS 协议发送到认证服务器进行认证，如果是合法用户则可以访问网络资源，否则就会被拒绝在外。

目前支持的防火墙和 VPN 厂商包括 Checkpoint/Norkia、Netscreen、Nortel 和 Cisco 等 IPSec VPN 厂商以及 Juniper、F5 等 SSL VPN 厂商。

4.2.5 Web 服务器保护

Extranet 已经成为电子商务的关键部分，它使得客户、合作伙伴和供应商进行交流成为可能。SafeNet OTP Client for IIS 的功能就像安全警卫，充当一个 URL 过滤器，代理软件截取访问请求并且要求指定的用户或组在获得受保护的网站资源访问许可之前，使用认证设

备到后台认证服务器进行认证。另外，您可以自己控制用户权限，决定用户被认证通过以后，是否能够访问这些资源。

4.2.6 Oracle 数据库保护

Oracle 是全球领先的信息管理软件的供应商，由其提供的 Advanced Security Option（ASO）软件保护 SQL*Net 和 Net 8 环境下的敏感的以及有价值的信息。当用户试图访问 Oracle 数据库时，Advanced Security Option 软件加密并且执行安全检查。SafeNet 使用预先发给每个用户的 eToken 令牌认证用户的身份。使用 Oracle 的 Advanced Security Option 和 SafeNet eToken 令牌，所有基于 Oracle 数据库的网络应用程序均可以得到由 SafeNet etoken 令牌提供的强用户认证。

4.2.7 使用 RADIUS 协议与应用程序集成

企业中存在大量的应用，这些应用程序可能是基于 B/S 架构，也可能是基于传统的 C/S 架构，这些应用中包含着企业的重要数据和资料，同样需要进行安全有效的保护，确保访问用户身份的真实性并且赋予相应的访问权限。

SafeNet eToken 双因素验证解决方案提供一次性密码的支持，在验证服务器端可以安装 eToken Radius 服务器，此服务器读取微软 Windows 活动目录中用户信息，并且通过保存在活动目录中的令牌种子运算出令牌当前的一次性密码，与用户输入的一次性密码进行比较，如果相同的话即证明此用户为合法用户。

原有的认证方式应该都是基于数据库的用户名和静态口令认证。需要用户在客户端输入用户名和静态密码，认证信息发送到服务器端，服务器端软件通过数据库查询的方式和数据库中的密码字段比对，如果完全一样的话就是合法用户。

现在需要对客户端和服务器做适当的修改，允许用户在客户端输入 PIN 码加上一次性密码，用户点击确认键以后这些认证信息发送到服务器端，服务器端通过 RADIUS 标准协议发送到 SafeNet 认证服务器上进行认证，并且获得一个返回结果，通过认证的用户才是合法用户。

目前 eToken Radius 服务器支持标准的 Radius 2865 规范，只要遵从此规范的身份验证信息均可以和 eToken Radius 服务器无缝集成。如果需要在应用服务器端嵌入 RADIUS 标准认证的话，不是很困难，只需要从网络上获得此规范，然后按照此规范的要求实现 Radius 通讯代码即可，最简单的实现只需要发送一个认证消息并且获得结果即能够实现认证。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

对于那些 B/S 架构的应用来说，可以使用 eToken OTP Client for Web 来进行保护，用户访问关键应用页面的时候会弹出身份验证页面，通过了 eToken 一次性密码验证以后才能够安全访问应用，也可以使用自己开发 Radius 客户端，将身份验证嵌入到应用程序中。用户可以在这两种方式中自由选择。

4.2.8 认证服务器的容错

由于会在关键的应用中使用双因素认证，如果后台认证服务器死机，所有的用户均无法访问这些资源，给用户的使用带来很大不便，所以为了减少停机的可能，至少应该安装两台认证服务器，任何一台服务器的发生故障的话不会影响整个认证过程。

4.2.9 详细的报表和事件跟踪功能

对于用户的每一次认证企图和通过管理程序做的任何动作，都会在后台认证服务器的日志中产生相应的一条记录，管理员可以运行大量的报告来查账审计。

第三方的日志管理工具实时采集 Event Log 中的认证信息，以最快的速度响应系统问题。

4.3 选择适合您的设备

eToken 系列设备可以完整灵活地迎合客户不同地要求，从 PC 登录、远程登录到基于智能卡的访问控制和身份认证，eToken 都能实现。今天，为了不断变化的数字时代始终保持领先优势，高效与便捷是一个商业人士的明智选择。eToken 通过标准化接口，能够与第三方安全系统实现无缝结合。

eToken 可以实现靠近式整体解决方案，可以将接触式与非接触式两者整合在一起，实现物理的楼宇访问与逻辑的数字资产的访问实现完美的结合。

4.4 服务器部署和选择

TMS 服务器需要安装在 Windows AD 环境中，如果企业已经拥有 AD 环境的话，可以直接将 TMS 安装在现有环境下；如果暂时还没有 AD 环境，应该首先创建 AD，在创建 AD 时需要考虑域名、用户如何分组、用户帐号如何命名以及用户密码策略等相关问题。

在安装 TMS 时，不一定需要安装在 AD 域控制中，可以安装在加入域的的一台成员服务器上。由于负载不是很高，可以选择普通的服务器进行安装，以下是推荐的服务器硬件配置：

- Intel CPU 1.8GHz 以上
- 2G 内存
- 1G 空余硬盘空间

TMS 所有的管理功能均通过 Web 界面完成，所以管理员可以在企业任何计算机上通过浏览器即可实现对 TMS 服务器的管理。

4.5 数字证书身份验证实施

有多种方式可以实现身份验证，目前市场上主流的双因素身份验证方式是数字证书认证和一次性密码认证。以下是两种不同认证方式的比较：

	令牌 （OTP）	USB Key + 数字证书

初始成本	客户需要购买令牌以及相应数量的服务器用户授权	如果使用数字证书方式进行认证的话，用户只需要购买 USB 令牌即可，配合微软的证书服务器（完全免费）来实现双因素认证，没有服务器端的费用，同时单个 USB 令牌的价格也要比 OTP 令牌便宜许多，所以整个初始成本可以非常低。
令牌有效期	OTP 令牌一般有时间限制，从 2 年到 5 年不等，当令牌超过有效期以后，用户必须重新购买新的令牌来替换过期的令牌，带来很大的费用负担	USB 接口没有时间限制，客户可以永久拥有此硬件认证设备
使用方便性	每次认证的时候都需要手工输入 PIN 码和令牌码，使用起来比较繁琐。如果需要登录多个使用 OPT 保护的应用程序时，时间同步令牌每次认证完毕都要等待一分钟才能登录下一个应用。	只需要在每次开机的时候插入 USB Key 并且输入 PIN 码，每次认证的时候应用程序会自动到 USB Key 中读取相应的凭证，不再需要用户手工输入任何信息
单点登录功能	使用令牌无法实现单点登录，用户每次认证时都需要输入认证信息；或者需要购买专门的单点登录软件来实现	无论是 C/S 或者 B/S 应用程序，在 USB Key 中可以保存这些第三方应用程序的静态口令，当用户启动这些应用程序的时候，可以将登录凭证自动填入登录界面，实现应用程序的自动登录；对于应用程序来说不需要做任何修改
令牌种子的安全性	一般令牌在出厂时会将种子植入令牌，厂商知道每块令牌的种子值，存在一定的安全隐患；同时，这些令牌的种子值以明文的方式传送给客户管理员，在运送过程中也容易泄漏种子值。	管理员为每个用户申请并导入发放数字证书，安全地存放在 USB Key 中，这个过程完全由管理员来控制，杜绝了其中的安全隐患。
对信息安全的整体保护	仅仅实现身份认证功能	除了实现身份认证功能以外，还可以实现数据的私密性、完整性和不可否认性。

综上所述，功能上来 USB 加数字证书具有更大的优势。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室　(200233)
电话：8621-64701090　　传真：8621-54640133-803
E-mail：jackwrw@msn.com　网址：http://www.wang-cai.com
免费电话：400-600-9103

为了实现 PKI 应用，需要在企业中建立一套 CA 认证中心。可以选择 Windows 操作系统中自带的证书服务器，SafeNet TMS 提供专门针对于 Microsoft CA 的连接器，当在 TMS 中注册令牌时，TMS 可以代替用户的身份到 Microsoft CA 上申请证书，然后将获得的证书自动安装到用户的 eToken 中，轻松实现数字证书的颁发。

用户可以使用颁发的数字证书实现各种 PKI 功能，包括访问 Windows 操作系统和应用的强身份验证、交易的签名和加密、针对文件夹和硬盘的加密等应用。所有需要使用 eToken 的客户端必须首先安装 PKI Client，PKI Client 的功能主要是驱动所有类型的 eToken 设备，同时提供 PKCS ＃11 和 CAPI 接口给应用程序方便地调用 eToken 的数字证书进行 PKI 操作。

对于那些可以由用户自己完成，不需要管理员介入的操作，例如令牌注册或者密码重设，可以使用用户自助服务来实现，帮助企业节省大量的时间和成本。用户可以快速地处理他们自己的令牌，增强了生产效率同时减轻了 IT 管理员的负担。令牌管理系统提供提供的 Web 界面可以进行定制，提供企业用户最大的灵活性。所有使用 TMS Web 自助服务平台的用户必须在客户端安装 TMS Client 软件。

客户端软件例如 PKI Client 和 TMS Client 软件均可以通过软件分发分发工具（微软 SMS）进行分发和安装。

整个项目的实施过程如下：

- 安装 Microsoft 证书颁发机构企业版
- 配置 Microsoft 证书颁发机构发布相关的证书模板
- 安装 TMS 服务器软件
- 配置 TMS 服务器组件中 Microsoft 颁发机构连接器
- 用户登录 TMS 自助服务器平台或者管理员代替用户到 TMS 服务器上注册令牌
- 在令牌注册过程中 Microsoft 颁发机构连接器会自动到 Microsoft 证书颁发机构申请证书，自动保存在用户的 eToken 中
- 用户使用自己的 eToken，可以使用其中的数字证书登录域环境、访问 Web 应用以及建立 VPN 加密通道。

4.6 一次性密码身份验证实施

一次性密码认证解决方案使用一次性密码来登录网络，无论您处于何时何地，完全不需要安装客户端软件或者使用 USB 连接。此解决方案基于 eToken NG-OTP 设备。

eToken 一次性密码认证架构包括 eToken 一次性密码认证 RADIUS 服务器实现后台的一次性密码认证。允许与任何内置 RADIUS 认证接口的安全网关/应用集成，包括领先的 VPN 解决方案、Web 访问解决方案等等。

一次性密码认证解决方案由令牌管理系统进行管理，其还可以实现完整的企业级令牌部

署和生命周期管理。 eToken RADIUS 服务器利用活动目录基础架构来获得用户信息。

整个项目的实施过程如下：

- 在现有的 Microsoft Active Directory 上安装 SafeNet TMS 服务器。
- 在域控制器上安装 Microsoft IAS Radius 服务器
- 安装 SafeNet eToken IAS 插件，配置此插件使用 SafeNet eToken 进行认证，没有分配 eToken 的用户可以暂时使用 Active Directory 中的用户名和静态密码认证
- 配置 VPN 网关，使用外部认证服务器，使用 RADIUS 认证协议将认证请求发送至 Microsoft IAS
- 测试用户使用 SafeNet eToken 一次性密码进行认证
- 将应用程序切换到 RADIUS 认证，测试使用一次性密码进行认证

4.7 密码管理 — 企业级单点登录

您的企业是否同样碰到以下有关密码管理的问题：

- 多少次您的用户为了不忘记密码而将他们的密码写在纸条上，放在皮夹中或者贴在计算机屏幕上？
- 您的用户是否为了方便记忆密码而对多个应用程序使用相同的密码？
- 您的帮助台支持人员是否将大量宝贵的时间和资源用在解决与密码相关的问题上？

用户现在可在单个 SafeNet eToken 设备中安全地存储和管理其所有计算机登录凭据。用户所需要做的只是记住一个 eToken 密码。您可以确保只有经过授权的人员才能访问组织的网络和资源。结果如何？结果是提高的生产力、降低的帮助台成本以及更好的安全性。

SafeNet 的单点登录解决方案提供用户 3 种模块可供选择：

eToken SSO —— 企业级的单点登录

有效地管理各种 Windows 应用程序的登录凭证，包括各种 B/S 以及 C/S 架构的应用程序。在一个 eToken 上，安全地存储和管理用户所有的计算机应用程序登录凭证。使得 IT 管理人员可以确保只有获得授权的人员才可以访问公司的网络和受保护的应用程序。

eToken Web SSO —— 基于 Web 的单点登录

使用一个 eToken 可以安全地存储和管理所有的基于 Web 应用程序的登录凭证。能够直接从网页获取用户的登录和访问凭证，简单、便捷和安全。同时在 eToken 中可以存储所有登录信息，包括：密码、PIN 号、账号、信用卡信息、电话号码、URL、过期日期和帐单。自动识别保存的网页，然后提交。使用户能够安全直接地访问他们所有的网络账号。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

eToken GINA SSO —— 安全的网络登录

安全地管理操作系统的登录凭证，使得网络管理员可以对 Windows 登录施行双要素用户验证，当用户登录操作系统时，必须插入存放 Windows 操作系统用户名和密码的 eToken 并且正确输入了 eToken 的密码以后才可以安全的登录操作系统。

eToken 单点登录方案能够方便、安全地存储用户的所有应用程序登录帐号，用户只需要插入 eToken 并输入 eToken 密码，就可以登录到公司网络、VPN 或任何有密码保护的应用程序。使用 eToken 为身份验证过程增加了一层额外的安全性，它要求用户同时出示 eToken 以及 eToken 密码才能允许进行访问，从而实现了真正的双要素身份验证。IT 管理员能够确保只有经过授权的人员才可以访问企业的网络和受保护的应用程序，不但提高了效率，减少了 IT 时间和成本，还获得了更高的安全性。

eToken 网络登录程序，存储用户名、密码和域名的组合，然后与微软网络登录(GINA)机制进行通信。为了进一步提高安全性，可以使用随机生成的密码，用户自己都不知道它们。

单点登录方案的优势

- ✧ 增强对您的企业的 IT 资源和知识财产的安全保护
- ✧ 提高雇员的生产力，用户不需要花费大量的时间和精力用来记忆密码
- ✧ 为用户登录凭证提供了便携性
- ✧ 强大的双要素身份验证机制，在安装了 GINA 的单点登录客户端软件以后，可以配置此客户端必须使用 eToken 才能够登录操作系统，即使用户知道了此操作系统的用户名和密码，也无法直接登录到此操作系统。
- ✧ 用户在修改应用程序的密码的时候，可以让 SSO 客户端程序自动产生一个复杂的密码填入应用程序中，这样的密码可以完全保证其安全性，不可能被破解，同时用户也不知道真实的应用程序密码，每次登录应用的时候必须插入 eToken
- ✧ 可以强制推行 IT 安全策略，在保存用户的应用程序密码的之前，可以首先检查此密码的安全等级，不符合安全的密码不允许存储到 eToken 上，增加了应用程序的安全性

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103

- ✧ 降低密码管理的成本
- ✧ 最少的 IT 援助和维护
- ✧ eToken 激活了多种其它的安全服务

eToken SSO 保存登录凭据，并在用户使用 eToken 通过强身份验证之后自动提交凭证，从而使用户可轻松访问他们所有的计算机应用程序。

除了为用户提供了安全便捷的访问工具之外，eToken SSO 还提供了直观、易用的管理工具，以使您能够完全用户的 SSO 使用情况，并实现使用 eToken 安全地访问自建应用程序。

eToken SSO 完全与 SafeNet Token Management System (TMS) 集成，TMS 为管理员提供了一整套令牌管理服务，包括 eToken 部署和撤消、用户自助式密码重置以及备份/恢复丢失或损坏的令牌的用户凭据。

5 SafeNet 解决方案优势

- ✧ SafeNet 所有系列的智能卡设备均配有智能卡芯片，可以同时支持数字证书的强身份验证、数据的加密保护以及密码管理功能等安全应用
- ✧ SafeNet 是全球 USB 和智能卡技术的领导者，在 USB 市场占有最大的市场份额，同时拥有众多 USB 专利技术。
- ✧ 可以同时支持一次性口令（OTP）与数字证书两种认证技术。可以集成 PKI 功能、一次性密码认证和门襟系统访问于一身，最大限度保护了客户投资。
- ✧ SafeNet eToken 提供最大的灵活性，可以根据客户的要求丝印上或者铭刻客户的商标 Logo 实现定制。
- ✧ 紧密集成微软的目录服务器，管理员在同一个活动目录管理界面中，可以管理所有用户帐号，认证设备以及所有的安全应用，而不需要在多个管理界面中切换。
- ✧ SafeNet eToken 完美集成了物理访问和逻辑访问，用户仅需要使用同一个凭证。
- ✧ 使用 SafeNet eToken USB 设备不需要智能卡读写器，可以节省智能卡读写器的投资。
- ✧ SafeNet eToken 可以实现完整的密码管理功能，安全地保存企业应用程序的登录凭证，当用户访问这些应用程序时可以自动登录，这些应用程序包括客户/服务器应用，Web 应用以及 Windows 操作系统登录。
- ✧ 获得全球 100 多家合作伙伴厂商的支持，eToken 可以配合 VPN 远程接入、Windows 域登录、PKI 应用以及数据加密厂商等等。
- ✧ SafeNet 令牌没有使用年限的限制。
- ✧ 提供用户最好的性能价格比。

地址：上海市徐汇区桂林路 396 号 3 号楼 611 室 (200233)
电话：8621-64701090 传真：8621-54640133-803
E-mail：jackwrw@msn.com 网址：http://www.wang-cai.com
免费电话：400-600-9103