网管与 IT 运维

应用动态密码认证实现密码安全和强身份认证

技术建议方案

四川安盟电子信息安全有限责任公司

1 方案提出的政策和技术背景

1.1 国家重要信息系统等级保护条例

等级保护条例有关身份验证的要求概要如下：

1）应对登录系统的用户进行身份标识和鉴别；

2）用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

3）当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；

4）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，其中一种具有不可复制和篡改的特点。

《国家重要信息系统登记保护条例》由公安厅、信产部等推动，经过自我评估、第三方公司差距评测，目前已经进入到差距整改阶段，是国家强制执行的一项信息安全标准。

1.2 互联网的不安全性以及人的不可控因素

互联网具有完全开放的特性，在带来方便性和低成本的同时，大量的病毒、木马程序泛滥，黑客横行，几乎达到不可控制的程度，身份信息泄露，数据信息信息泄密成为新的安全风险。

多年的信息安全管理经验表明，信息安全管理中，人是最不可控的因素，人的安全意识、安全习惯和安全技术水平参差不齐，就密码安全来说，设置简单密码，密码长期不更新，多系统设置同样的密码成为常态，极易被猜测和盗用，导致泄密和受到黑客攻击。

一般而言，IT部门对于密码管理的要求如下：

（1）密码的长度足够长，至少 8 位

（2）数字和英文字母混合，大小写混合等

（3）必须定期更新，一般要求 1 个月更换一次

实际上，上述要求我们往往不能做到，主要是因为人的惰性、安全意识和可实现的问题，即使有做到上面的要求，我们的员工往往是将密码记录在自己的工作本后面，也只有这样才可能记住，但同时也带来的如被同事看到或者工作本丢失这样的风险问题。

而口令是网络信息系统最常用的安全与保密措施之一。如果用户采用了适当的口令，那么他的信息系统安全性将得到大大加强。但是，实际上网络用户中谨慎设置口令的用户却很少，这对计算机内信息的安全保护带来了很大的隐患。

此外，还可以从一个合法的终端上窃听会话并记录所使用的口令，采用这种方法，无论你所选择的口令如何好都无济于事。例如 HTTP 和 Telnet 协议都是不安全的网络协议，传输过程中不作任何加密，其他人只要在传输过程中安装 Sniffer 程序就可以非常方便地获得合法用户的口令就可以以非授权身份登录访问有关资源。

2 网管与 IT 运维关于强身份认证的需求分析

网络设备、服务器主机和数据库系统是企业业务和生产运营的 IT 支撑平台，其重要性毋庸置疑，对于这些网络设备的保护至关重要。如果非法用户获得管理员的帐号到网络设备上作了非法修改有可能导致整个网络系统的瘫痪，至企业的业务和生产运营停摆，所以有必要对进入网络设备进行配置的人员进行强认证。

同时，对于整个网络系统来说，有许多从互联网进入企业内部网络的接口，如拨号服务器、防火墙和 VPN 网关，我们知道互联网是非常不安全的，如果黑客获得了合法人员的口令就可以冒充合法人员进入企业内部网络，进入服务器主机和数据库系统，窃取关键的业务数据，对网络进行恶意破坏，这样企业就面临非常严重的后果，造成经济损失和企业商誉受损，以及主管部门的处罚。而对于哪些被盗取口令的用户，他们本身并不知觉，黑客每天都在冒充他的身份访问网络，最终的责任必定还是由自己承担。

另一个实际情况是，企业的 IT 平台维护往往由三部分人组成，一是企业自己的 IT 维护工程师，这部分人还比较好管理和控制；二是外包给第三方公司代维的工程师，他们不是企业的员工，人员具有流动性，不好管理；三是 IT 设备和软件的厂商工程师，这部分人更加具有流动性，可能每次来服务的工程师都不同。为工作的方便性，我们往往需要提供网络设备、服务器主机和数据库系统的最高权限的账户和密码给代维工程师和厂商工程师，但往往不会因为本次维护完成后即修改账户密码，这就有可能他们记住密码，从外部进入系统进行窃取数据和破坏，这是最大的风险。

目前网管和 IT 运维普遍采用 KVM 和堡垒机（IT 运维审计系统），这类系统一方面具有授权功能，成为网管和 IT 运维的门户，一方面具有审计功能，详细记录 IT 运维的操作行为。应用这些系统后，由于作了集中授权，非法获得 KVM 或者堡垒机的账户后，就全部获得了该账户的全部授权管理资源，因此增大的风险。

网管和 IT 运维的密码保护和实施强身份认证成为必然的选择。

3 技术建议方案

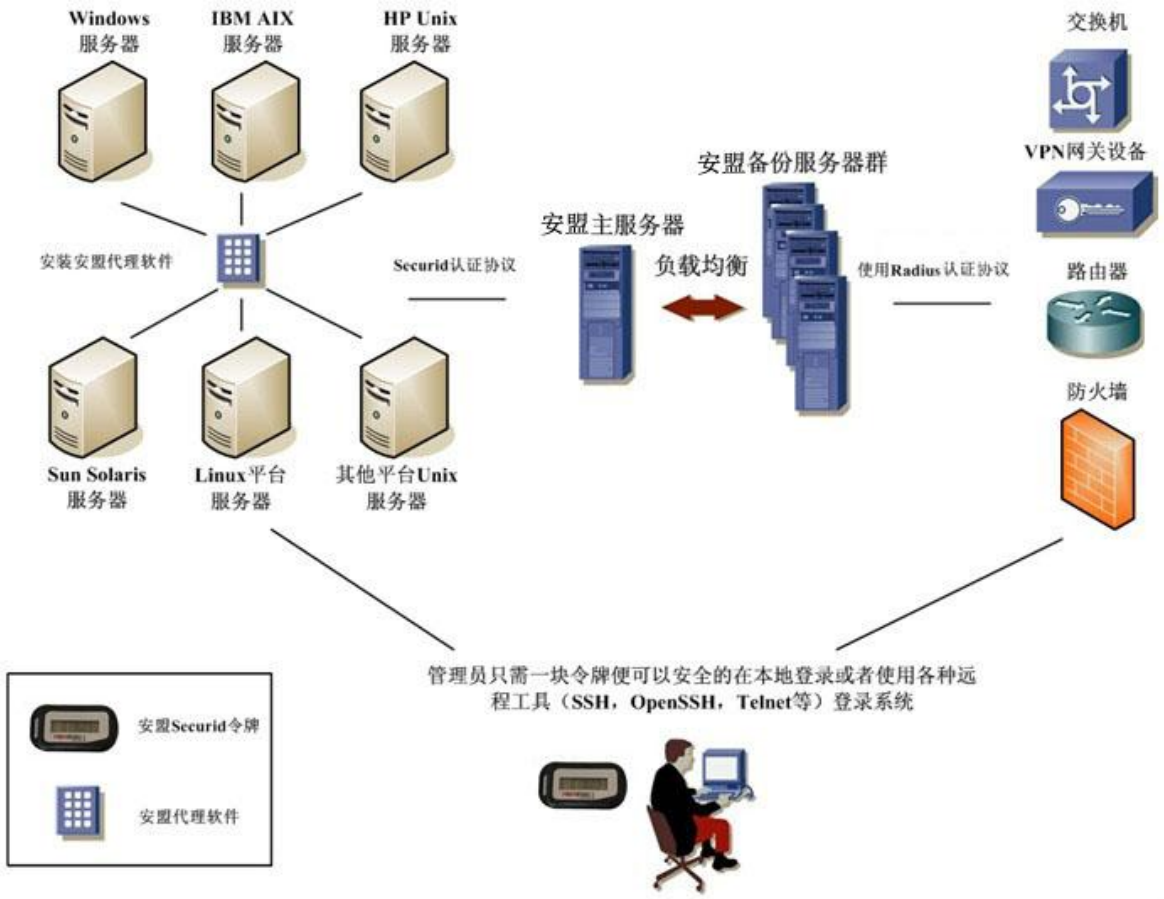
方案设计的主要依据如下：

（1） 根据《国家重要信息系统等级保护条例》，对于等保二级以上的系统，应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，其中一种具有不可复制和篡改。动态口令令牌作为不可复制和篡改的个人持有信物，通过与账户绑定后，能够作为有效身份信息。

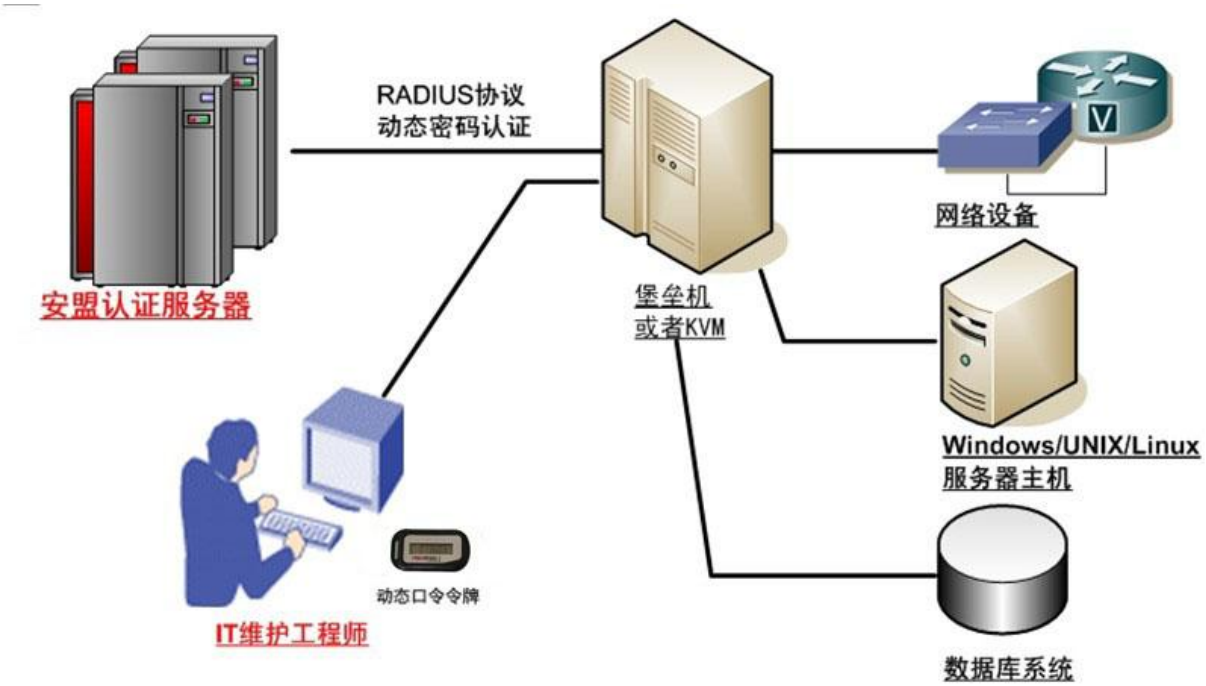
（2） 良好的用户体验。由于人的惰性，以及安全意识和习惯，不愿也不可能设置、记忆和定期更新密码，动态密码只需要用户持有令牌，并安全保管自己的令牌，既可实现密码安全。且登录过程也不改变原有的习惯。

（3） 动态密码是通过专用高强度加密算法计算得出，不可预测，只在一定期限内有效（一般 3 分钟），且使用一次即失效，具有足够的安全性。

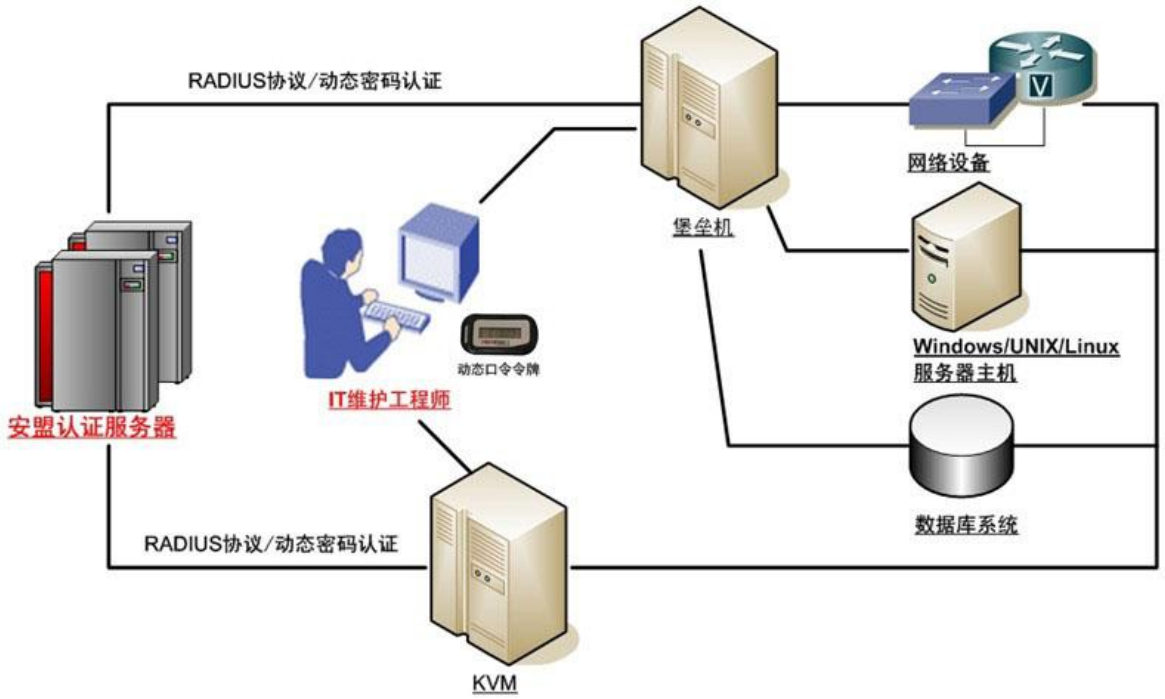
解决方案部署示意图如下：



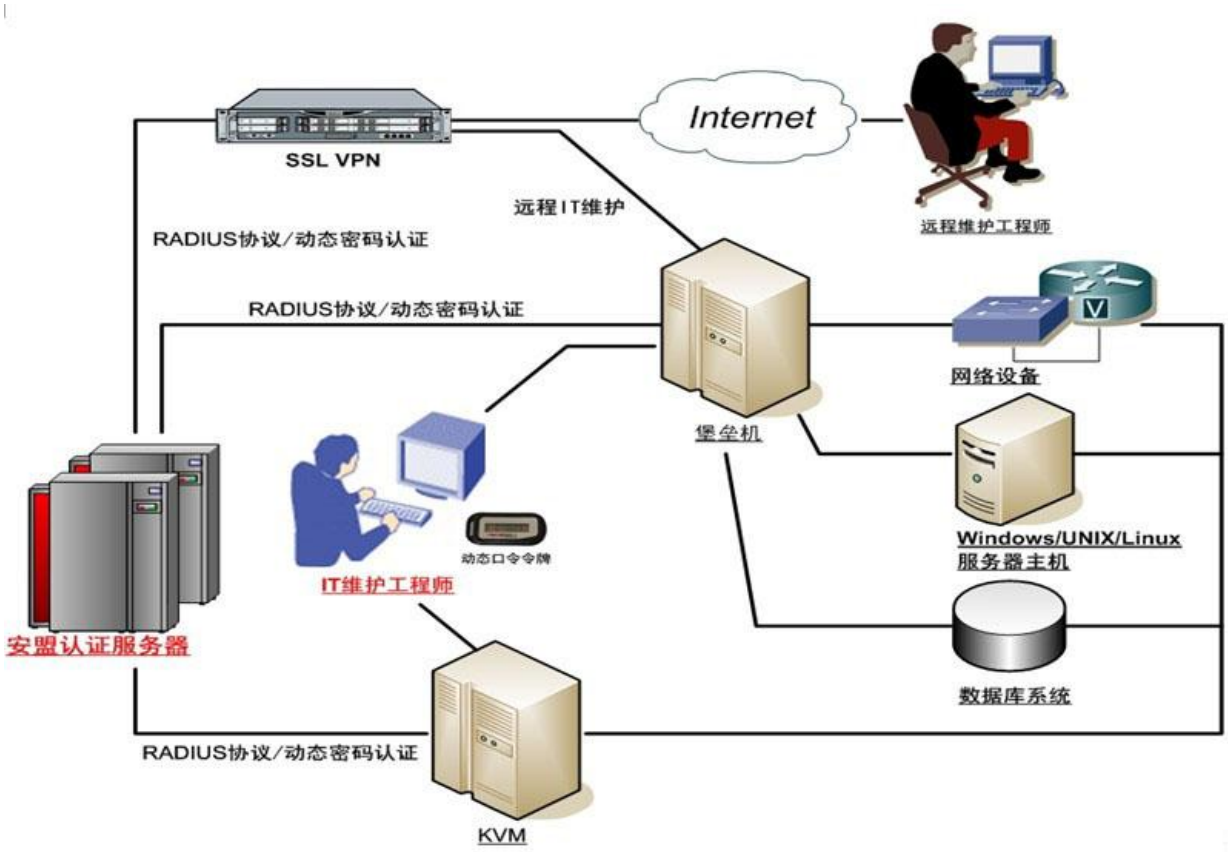
对于采用堡垒机或者 KVM 的情况，部署示意图如下：



对以同时采用堡垒机和 KVM 的情况，部署示意图如下：



对于采用堡垒机和 KVM，同时采用 VPN 作为远程维护的情况，部署示意图如下：



3.1 关于动态密码的安全性

（1） 动态口令采用伪随机算法，基于 128 位加密密钥和时间，每分钟产生一个完全不可预知的 6—8 位密码。并且，该令牌采用高强度加密算法，完全不可复制和篡改，具有完全的安全性。

（2） 动态密码是通过专用加密算法计算得出，不可预测，只在一定期限内有效（一般 3 分钟），且使用一次即失效，具有足够的安全性。

（3） 用户只需要持有动态密码令牌，并安全保管自己的令牌，既可实现密码安全。

3.2 关于用户体验

关于用户体验方面，动态口令认证体现在以下几个方面：

（1） 符合人的使用习惯：由于人的惰性，以及安全意识和习惯，人们不愿也不可能设置、记忆和定期更新密码，而本方面只需要用户持有并妥善保管好自己的令牌，既可实现密码安全，且登录过程也不改变原有的习惯，即只需要在原登录过程中增加动态口令输入即可，不需要特殊的 IT 知识和技能。

（2） 一个用户只需要持有一个令牌，即可登录其拥有账户权限的所有系统。令牌是人的第二沈身份信息，可以在认证服务器与该账户拥有权限的多个应用系统绑定，实现在后台的统一授权。

3.3 关于操作责任厘清

关于操作责任问题，由于密码的产生在用户的令牌上，而令牌已经以正式和严肃的方式发放给用户，只有用户才可能获得密码，管理方不可能生成和获得该密码，因此输入正确密码就可以确认交易方身份的唯一性，用户方是不可推卸责任的，可以防止抵赖行为。

3.4 关于与应用系统的整合

主要通过以下三种方式解决：

（1） RADIUS 协议，适用范围包括网络设备、安全设备等，以及 ORACLE 数据库等。

（2） SecurID 协议，适用范围包括支持 SecurID 认证协议的应用系统，如 SAP（需要部署认证管理模块）、IBM Tivoli 门户系统等）。

（3） 安盟认证代理，适用范围包括服务器主机（Windows 系列、UNIX/Linux 系列）。

3.5 适用的范围

（1） 网络设备

网络设备都支持 Radius、SecurID 认证协议实现第三方认证，安盟认证服务器支持上述协议，部署时只需在网络设备上将认证模式选择为 RADIUS 或者 SecurID，将认证服务器 IP 地址指向安盟认证服务器的 IP 地址，并制定相应的端口即可，管理员使用远程登录工具或者本地登录都需要输入动态口令才能进入系统。

（2） 服务器主机

Windows 全系列操作系统，支持 32/64 位。

Linux 各厂商的所有版本。

UNIX 各厂商的所有版本。

（3） 数据库系统

ORACLE 9i 以上的版本支持 RADIUS 协议，其他的数据库系统需要安装安盟认证代理实现。

3.5 方案实施后的意义

1）从技术层面加强机房网管与 IT 运维的安全性。

2）解决了密码安全管理的问题，安全性不再依赖个人的安全意识和习惯，实现可控的安全性。

3）良好的用户体验，用户不再发愁设置、更新复杂密码，且只需要携带动态密码令牌即可。

4）符合《国家重要信息系统等级保护条例》以及行业安全生产的有关规定和要求。

4 关于安盟动态密码双因素强身份认证系统

动态口令技术最常见的就是 SecurID 技术，其基本原理就是在认证服务器和每个用户分别共享一个对称密钥，每个用户都有一个 PIN 码。用户持有一个硬件令牌，该令牌包括密码芯片（存储那个对称密钥）、一个时间源芯片、一个电源和一个液晶现实芯片。该令牌和认证服务器一般以该密钥和时间为基础，每隔一定时间（常见为 60 妙）就计算出一个口令，由于令牌和认证服务器双方都共享了对称密钥、时间因子和计算方法，所以分别计算出来的口令就是同步的。用户根据的令牌计算出来的口令，自己在客户端输入自己的 PIN 码和口令，客户端把这些信息传送到认证服务器，根据用户账号和口令来对该用户进行认证。

在这个认证过程中，有一个显著的特点就是令牌和认证服务器之间没有交互，而且由于认证所使用的口令的产生，令牌和认证服务器共享的对称密钥时间有关，所以是一次一密方式的认证，认证过程就是口令的比对，所以认证所需要的资源十分有限，同时由于一次一密和必须同时拥有令牌的特点，属于双因素认证，因此属于高强度的认证方式。

4.1 动态口令身份认证系统原理

在传统的静态口令验证系统中，由于口令为“一次设置，重复使用”，由于口令的重复使用而增加了口令丢失和破解的危险性，降低了系统的安全系数，特别是在互联网环境下，黑客、木马和病毒泛滥，使得静态口令更加容易被泄露，造成企业信息系统和资源的非授权访问，导致直接经济损失和间接的信誉和商誉损失。

所以，除了用户记忆的静态口令外，还需要增加一个物理因素，如令牌，这样采用你所知道的（记忆的静态密码）和你所拥有的（令牌）两个要素构成有效密码，实现严格身份信息验证，而你所拥有的要素必须具有不可复制和篡改的性能。

动态口令认证即是依据上述原理实现的双因素强身份认证系统：

1) 本系统以令牌作为信物，实现双因素认证。令牌显示依据种子密钥和时间随机计算的动态口令，具有不可复制和篡改的性能，而后台认证系统认为，只有持有令牌才可能输入正确的密码，反过来说，只要输入了当前时间点的正确密码，就可以认为持有可信的要素，即令牌。用户登录时，必须同时验证静态口令（称之为 PIN 码）和动态口令，只有两者均正确时才能确认用户身份

2) 令牌与服务器之间的同步。令牌和认证服务器一般以密钥和时间为基础，每隔一定时间（常见为 60 妙）就计算出一个口令，由于令牌和认证服务器双方都共享了对称密钥、时间因子和计算方法，所以计算出来的口令就是同步的和唯一的。

3) 一次一密。令牌上显示的密码只在当前时间点有效，且使用一次即失效，实现高强度的安全性。

解决的主要问题：

1) 密码安全管理问题，实现不依赖于客户端安全意识和安全习惯可控的安全性，用户也免于设置复杂密码、记忆并定期更新之苦。

2) 密码每分钟变化，只在当前时间点有效，且使用一次即失效，即使黑客在传输过程当中截获或窃听了，只有在一分钟之内解开，且解开之后，必须先于用户或管理员进入系统才构成威胁，这几乎不可能，大大加强了应用系统的安全性和可靠性。

3) 通过安盟认证器的日志审计系统可以对所有登录用户的信息进行记录，如用户的登录时间，登录的用户名，使用的哪一块令牌，从而可以确认用户的身份。

4.2 安盟身份认证系统组成

整个安盟身份认证系统由三部分组成的：

1）安盟 SecurID 身份认证令牌

令牌是分发给最终用户的，用以证明其身份的硬件或软件设备，是安盟双因素身份认证的一个因素（您所持有的），产生一分钟变化一次的动态令牌码，简单易用，便于随身携带。令牌每一分钟生成一个唯一识别用户的、无法预知的动态一次性口令。其硬件和软件版本都具有防篡改能力。如果某个用户提供了一个正确的令牌代码，就可以高度确信该用户就是拥有安盟 SecurID 身份认证令牌的合法用户。每个身份认证令牌拥有一个唯一的种子号，种子号是区分身份认证令牌的根本方法。一个用户可以绑定多个身份认证令牌（最多三块）。

安盟公司提供的身份认证令牌在产品设计、生产、运输等过程中严格按照国际标准执行，产品符合：ISO 13491-1：银行-安全加解密设备、ISO 8732(密码生成)、ANSI*9.32(数据加密标准)、ISO 11568(密

匙管理)、ISO 9797(消息认证码，MAC)。以及 EN61000-6-2 标准、Method RS101，MIL-STD-461D、EN55022 标准、ISO7816-1 等。

2）安盟身份认证代理软件

安盟身份认证代理软件实施安盟身份认证服务器软件建立的安全策略，在用户和被保护的资源和设备之间，通过安盟身份认证服务器软件来强制实施双因素认证。要求指定用户或组织在获准访问被保护的企业 Intranet 资源之前，通过一个安盟 SecurID 身份认证令牌向安盟身份认证服务器软件证明其合法身份。在用户和被保护资源及设备之间，通过安盟身份认证服务器软件强制实施双因素身份认证。安盟身份认证代理软件与安盟身份认证服务器软件之间的通信是通过加密传输的。是公共密钥技术的自然补充，对于保护宝贵的或受限的信息尤为有效。现有的主流网络设备已预装，具有较强的互操作性。支持现有的大多数主流平台。配置过程简单，易于安装、运行。

安盟身份认证代理软件 API SDK 使用户能够创建定制代理，从而保护其他面向特定的内部应用。

3）安盟身份认证服务器软件

安盟身份认证服务器软件是安盟 SecurID 双因素身份认证解决方案中的安全服务器，包括三个主要部分：包含用户、令牌和客户机信息的数据库；身份认证引擎以及一个管理程序。安盟身份认证服务器软件用来在选定的网络资源周围建立一个保护环境，对要求访问企业 Intranet 资源的各种用户进行身份认证。除了处理用户的访问请求认证，安盟身份认证服务器软件还可进行企业网安全策略管理，它提供了集中式安全管理能力，向信任的个人签发认证令牌证；设置并实施安全策略，保护对专用网络系统、文件及应用的访问，其中包括可以根据每天的时间、星期几或根据小组或用户定义的权限来确定访问权限；创建用户访问日志，进行审计跟踪；定义和报告报警情况，如某个网络端口访问失败重试次数等。安盟身份认证服务器软件可运行于多种服务器平台上，能够提供强大的认证服务。

4.3 安全性体系设计

安盟身份认证系统采用基于 AES 的循环加密法来生产动态口令，采用该算法生成的动态口令具有不可预见性，由于安盟的动态口令为 6~8 位，因此，同一时间产生相同动态口令的概率为 10^{-8} 到 10^{-6}，考虑到用户 4~8 位的 PIN 码，同一时间产生相同双因素动态口令的概率将下降为 10^{-16} 到 10^{-10}。

4.3.1 双因素认证机制

安盟双因素认证系统采用双因素认证机制来鉴别用户身份。用户登录时，除了一个记忆在头脑中的口令外，还必须提供他拥有的令牌所生成的动态。只有同时使用正确的用户 PIN 码和用户本人的动态口令令牌才有可能进入网络，使网络安全性大大提高。

4.3.2 令牌的唯一性和安全性

借助强大的用户认证系统安盟安全解决方案，可以向授权的员工发放单独登记的设备，以生成个人使用的令牌口令，这一口令可以根据时间而变化。每 60 秒就会生成一个不同的令牌口令，保护网络

的认证服务器能够验证这个变化的口令是否有效。每个认证设备都是唯一的。别人不能通过记录以前的令牌口令来预测将来的口令值。这样，如果某个用户提供了一个正确的令牌口令，就可以高度确信该用户即是拥有安盟认证令牌的合法用户。

4.3.3 一次一密认证机制

认证服务器对访问服务器送来的动态口令，进行一次一密认证。即使黑客通过工具截获使用过的认证信息令牌码，安盟身份认证系统也有效防止口令的重发攻击。

4.3.4 身份鉴别处理

安盟双因素身份认证产品提供了身份鉴别失败的处理功能。当用户以失败的身份鉴别尝试达到规定的数值时，能够及时终止用户与系统之间的会话过程，将用户帐号锁定，同时在系统登录日志中对身份鉴别失败事件进行审计跟踪。只有以授权的身份才能对审计跟踪信息进行修改和删除。

安盟双因素身份认证产品提供了有效鉴的鉴别信息，包括用户名和口令通行码（PIN 码+令牌码），每个授权用户都有唯一的用户名和唯一的口令通行码。用户的口令通行码是一次性的口令，且是不可伪造的。

在用户请求登录访问系统资源时进行身份鉴别，系统要求用户输入自己的用户名和通行码，只有正确的身份才能登录访问系统资源，否则系统拒绝访问。另外，安盟认证代理软件提供了一个符合规范的身份鉴别过程的用户界面，避免了用户的偶然泄密。无论用户以成功的身份还是失败的身份进行鉴别，系统对身份鉴别结果都进行了审计跟踪，并且保存在安盟认证服务器系统登录日志中，未被授权的用户不能更改审计跟踪的信息。