

Actividentity™

银行柜员动态口令身份认证系统

解决方案

Chicti  **n**

北京启迅网安科技有限公司

目录

前 言	3
第一章 银行业务系统背景	4
第二章 动态口令身份认证系统概述	6
2.1 系统登录	6
2.2 业务授权	6
2.3 轮岗管理	7
第三章 系统方案	8
3.1 认证机制及算法原理	8
3.2 ActivIdentity 令牌	9
3.3 认证系统拓扑图	10
3.4 认证流程	11
3.5 令牌发放，部署和管理	11
3.6 故障/应急处理	12
3.7 认证数据传递的安全性	13
3.8 日志和审计信息	13
3.9 安全管理制度	14
第四章 综述	15

前 言

随着电子化，网络化与信息技术的飞速发展，计算机技术在社会生活各个领域应用的不断深入，银行业务的基础设备跨越传统的局域网和广域网，电子化程度越来越高，从而充分利用网络系统的强大功能。在这种环境下，银行对计算机系统的依赖性越来越大。这就意味着银行需要向员工、承包商、业务合作伙伴和客户开放系统网络，其中包括核心业务数据及其他关键信息资源。因此，金融企业不得不面对这样的现实：信息系统工作空间已经不再完全处于信息系统或者本部门的完全控制之中。

在这种大环境下，金融领域的计算机和信息犯罪也随之出现不断增加的趋势，根据人行有关文件中的统计数字，近年金融计算机犯罪案件以每年两位数的速度递增。其中内部人员利用计算机犯罪，又占有很大的比重，近年来，国内一些银行先后出现了内部人员利用计算机犯罪的事件，不仅给银行造成巨大的经济损失，同时也对银行的声誉有非常恶劣的影响。

现在，银行正在建立先进的数字化安全系统，如防火墙，VPN 及 PKI 等基础安全设施。但如果没有对访问用户进行有效的识别和认证，这些安全措施最终也将形同虚设，其后果相当严重：经济损失巨大，关键行信息被破坏，品牌和声誉受损，核心业务注意力被分散等等。也就是说，银行业务系统安全的关键在于确切地了解谁正在访问系统，即身份认证。在这种情况下，需要根据受破坏的可能性，以及可能导致的损失，来评估预防措施的成本。

随着银行综合业务系统的推广使用，对柜员的身份验证和业务授权验证的安全性要求更高，管理工作也愈显迫切。人民银行就下发了《加强金融机构内部控制的指导原则》，提出了授权分责、一线岗位双职双责、建立后续监督机制等一系列的柜员内控管理原则。各大银行在银行综合业务系统的设计中，也为柜员内控设置了各种的安全措施，随着综合柜员制的出现，许多银行纷纷强化业务系统中的柜员身份认证方式。

身份认证的需求日益迫切，然而不幸的是，大多数银行业务系统所依赖的基于固定口令的身份认证机制既没有提供足够的安全访问控制，也没有在需要追查口令泄露责任时提供明确的用户帐号管理。同时，这种机制非常容易被攻破。

强大的身份认证安全解决方案是建立在双因素身份认证基础之上的。

第一章 银行业务系统背景

目前银行业务系统把各种业务分为普通业务和特殊业务两大类。普通业务是指普通的操作人员日常处理的金融业务，如储蓄开户，存取款等等。特殊业务则是要求有较高权限的操作人员(以下简称授权人员)进行授权才能处理的金融业务，如冻结，接冻结等等。也有些银行的业务系统将两大类业务再次细分，以区别不同的业务范围。

因此，现有银行业务系统把系统操作人员分按不同级别进行划分，以完成相应的级别和管理范围不同的业务。

目前，大多数的银行业务系统仍然采用基于固定的静态口令的身份认证机制，但这种机制在实际使用过程中存在不同程度的安全隐患。在很多情况下，口令泄露后，持有人并不能及时发现。而针对采用这种机制的系统，有多种手段与方式(如数据窃听，截取重放，字典攻击，穷举尝试等等)可导致身份认证控制失败。

在现实中，由于安全意识不足，在普通操作人员之间，个人在银行业务系统中的登录代码和口令都是相互透明的，很难保证不被某些别有用心的人员恶意盗用。由于口令没有载体，密码被盗用的事情就不能及时发现并进行有效防范和处理。

现有金融业务系统要求一个授权人员管理一个或数个营业网点，并负责对属于这些营业网点的特殊业务进行授权。在实际工作中，授权人员同时要负责其他业务和管理的工作，而特殊业务发生的时间和地点不确定，授权人员往往很难及时到达现场进行授权，因而往往将其授权代码和口令告知要求授权的普通操作人员。久而久之，这些授权代码和口令都成为不是秘密的秘密。显然，这种情况更是加大口令被恶意盗用的危险。

在某些金融业务系统中，普通操作人员需要在数个营业网店之间进行轮岗，为管理方便，轮岗人员在其轮岗网店内均有有效的授权身份(代码+口令)。显而易见，当该操作人员轮岗到一个网点时，轮岗的其他其他网点中的授权身份存在被恶意盗用的可能性。

针对固定口令机制的安全隐患，金融企业为此配合了相应的严格管理制度，例如，要求定期更换密码；规定“章随人走，卡不离身”；成立稽查部门对柜员遵守制度的情

况进行检查；对违反制度的柜员进行处罚等。这些管理制度虽然可以在一定程度上提高了系统的安全性，但并不能从根本上解决问题。柜员内控管理上的问题依然存在，如柜员临时离柜、业务授权人员临时有事离岗，节假日值班等情况，都可能在主观和客观上造成安全隐患，口令泄露引发的系统安全问题数不胜数；口令泄露后，对系统的侵入和攻击也不容易分清肇事者的责任。近年来，银行内部工作人员盗用他人密码，伪装身份访问超过自身权限的系统，非法窃取和挪用储户资金的案件时有发生，是每个银行都迫切需要解决的问题。

根据上述分析，金融业务系统需要更为完善的技术手段进行身份认证，以保障其安全性。

ActivIdentity 的银行柜员动态口令身份认证解决方案作为银行综合业务系统的内部管理子系统，可以为银行内部管理和银行业务管理系统提供安全可靠的身份认证支撑。

第二章 动态口令身份认证系统概述

ActivIdentity 动态口令身份认证解决方案,采用在现有的金融业务系统中应用动态口令令牌的方式,很好地解决现在固定口令机制的安全隐患。有一套完整的解决方案来为金融业务系统的柜员登录提供安全保障,例如:令牌产生的口令本身有 PIN 码保护;令牌持有人在令牌丢失后能立即挂失;他人不能同时得到令牌及 PIN 码,也就不能冒用令牌持有人的身份进入金融业务系统;令牌产生的密码不仅一次性有效,而且有使用时间的限制,不用担心被人盗用密码.....

在现有金融业务系统中应用动态口令身份认证解决方案,需要在操作人员的系统登录和业务授权两个阶段实施固定口令机制和基于“时间+事件”的动态口令双因素身份认证控制。同时,动态口令身份认证解决方案可以很好地解决操作人员轮岗时的安全问题,并能向所有的普通操作员和授权人员提供安全的保护机制。

2.1 系统登录

在操作人员的系统登录过程中,通过在登录窗口同时实施固定口令机制与基于“时间+事件”方式的动态口令两项认证。

首先,前台操作员必须要在登录窗口输入用户名,并且输入正确的固定口令。同时,还必须要知道所持有令牌的正确 PIN 码,把 PIN 码输入到令牌后,得到动态口令,把动态口令正确输入到登录窗口的动态口令提示窗口后,系统确认。才能接受操作人员的登录请求,通过业务系统的身份认证。

通过实施上述认证过程,金融业务系统确保了操作人员使用系统地合法性,安全性。并能正确确定操作人员的身份。

2.2 业务授权

在操作人员使用系统和处理业务的过程中,当其权限不足以完成某项业务功能时,可向相应授权人员申请对此项业务该笔交易的权限,例如当普通操作人员需要处理冻结业务时。

在实施完动态口令身份认证解决方案之后，业务授权流程如下：

- A、 前台操作人员用相应授权人员的授权代码和静态口令向业务系统申请该笔业务的授权；
- B、 若系统通过授权人员的授权代码和静态口令后，系统出现该业务所示界面，并提示输入授权人员的动态口令
- C、 前台操作人员向授权人员申请授权所需要的动态口令。
- D、 授权人员用自己所持有的令牌生成动态口令，并把动态口令数字告知前台操作员。

前台操作员在输入业务数据的同时，输入授权人员告知的动态密码。若动态密码正确，则系统提示业务完成；否则，系统提示授权不足或授权失败，退出业务处理流程。

上述认证流程，严格限定了业务授权的一次有效性，前台操作员在未取得授权的情况下，无法越权进行业务操作。授权人员的授权动态密码通过令牌产生，并且能够通过电话等远程方式把动态密码告知前台操作人员，前台操作人员在当次操作时密码有效，该笔业务操作完成后，动态密码即告失效。在保证操作便捷性的同时，也能满足授权业务安全性的要求。

2.3 轮岗管理

在实施动态口令身份认证的金融业务系统中，操作人员的授权身份与令牌是分开管理的，当某一操作员使用某一令牌时，只需要将授权身份所对应的用户名与相应的令牌做一个关联操作即可，系统根据授权用户身份对应的令牌来计算认证当时的动态口令，并以此来做身份验证。因此，当需要轮岗操作的时候，该类操作人员所持有的令牌对于其所有的授权身份都有效。

第三章 系统方案

3.1 认证机制及算法原理

在实施了动态口令身份认证解决方案的金融业务系统中，每一个员工都将手持一个令牌(令牌的详细资料见 3.2 ActivIdentity 令牌)。令牌内部有电池，处理器和存储器材，能依据出厂时内置的密钥，根据 ActivIdentity 独有的专利算法，用“时间”和“事件”参数，产生每次都不一样的密码。此密码一次有效，并且不会重复，无法推算，也不可通过逆运算计算出来。

当前台操作员需要访问业务系统时，系统界面会提示用户输入营业员代码(工号/用户名)，静态密码和动态密码。营业员首先在登录界面中输入营业员代码(工号/用户名)和静态密码，然后按动令牌按键，把令牌的电源打开。此时，令牌提示“Enter PIN”，营业员把自己记住的 PIN 码输入到令牌中，令牌的 LCD 即显示出一次性的，动态的口令。营业员把令牌中显示的动态口令输入到登录界面的动态口令一栏，再回车，即完成了全部认证过程。

营业员输入的用户名、静态密码和动态密码信息输入系统后，系统根据保存的该用户的相应令牌信息(时间/事件参数，初始化密钥，算法)计算出此时此刻用户应该具有的密码，并与用户送过来的密码进行比对。如果两者相同，则允许用户访问系统；如果两者不相同，则拒绝用户访问。

由于每一个令牌的初始化密钥都不相同，同时，初始化时候的时间/事件参数也不相同，而且时间参数随着时间不断变化，事件参数在用户每次正确输入 PIN 码的时候也自动加一。因此，保证了用户在任意时刻通过令牌产生的密码都是不相同的，也是不可复制，并且使用时间限制的。用户只有持有指定的令牌才能计算出正确的应答数以通过系统认证。以这个方法保证了用户是持有指定令牌的合法用户。

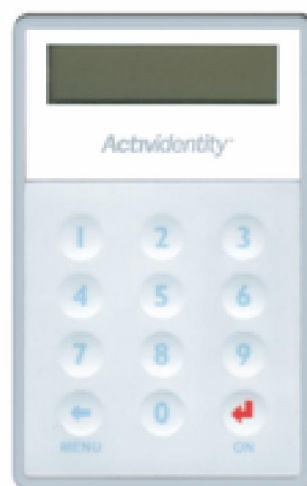
有五个方面来保证密码不被窃取：第一，令牌产生的动态密码本身被 PIN 码所保护，没有 PIN 码，非法使用者连密码都看不到。第二、动态密码根据变化的时间参数和事件参数经由只能被令牌本身读取的初始化密钥来产生，无法被反推算，或者穷举法等方法进行计算和破解；第三、动态密码使用一次后即告作废，及时在登录时被偷

窥或者嗅探，窃密者使用该密码再次登录，将被系统拒绝；第四，密码只在规定的时间内登录有效。在产生密码过后大约 10 分钟，系统将拒绝使用该密码登录；第五，在连续生成多个密码(<10 个)的时候，一旦用户使用序列中最后一个密码成功登录系统，则前面产生的密码都将被系统视为失效。从而，既防止了偷窥，也防止了网络嗅探等窃密行为。保证了很高的安全性。

3.2 ActivIdentity 令牌

提供安全服务：

- ü 同步认证(专利许可的时间+事件方式)
- ü 异步认证(挑战/应答)
- ü 简单的远程令牌管理方式
- ü 可定制的认证参数例如密码长度
- ü 数据证书
- ü 服务器认证



PIN 码管理

- ü PIN 码是由用户选择的且能随时更改。
- ü 设置 PIN 码输入保护并且能自动锁住
- ü 管理员通过 ActivCoupler (可选设备)进行初始化

令牌规格

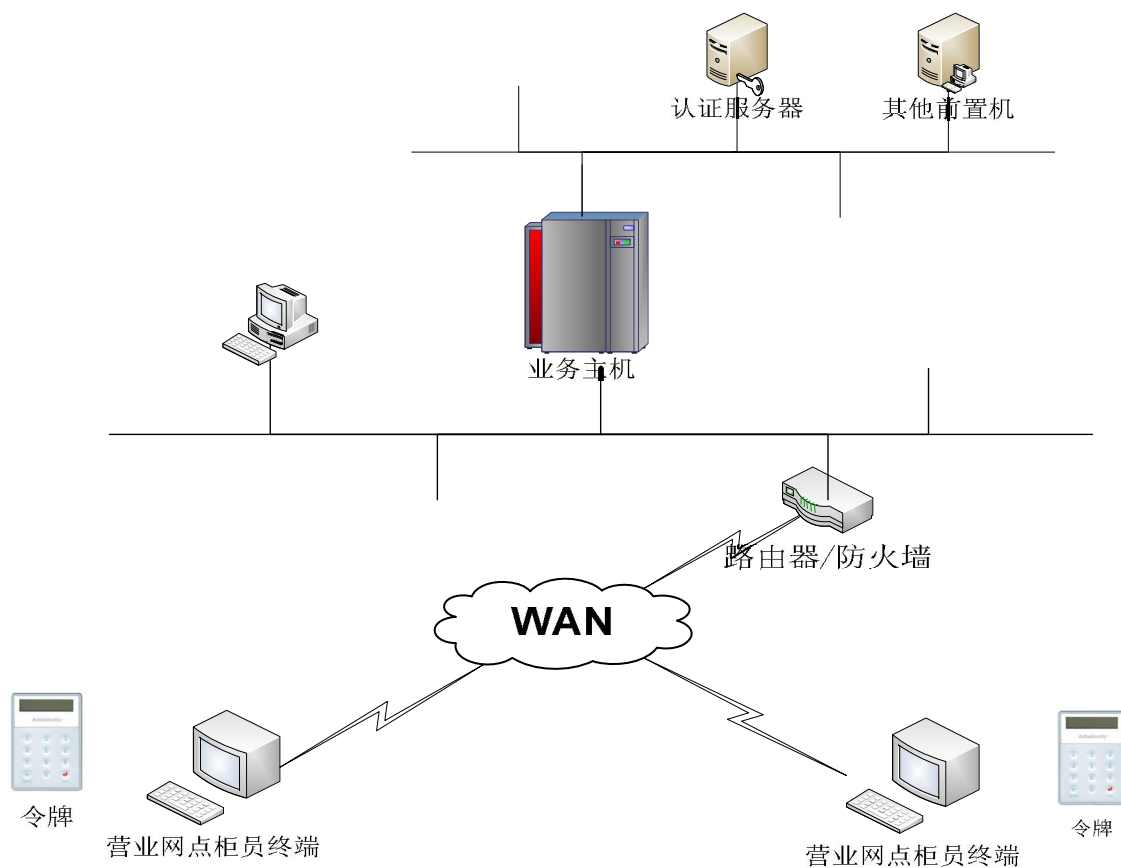
- ü 尺寸: 82mm x 52mm x 5mm
- ü 重量: 25 克
- ü 设计寿命: 8 年
- ü 12 键(10 个数字键和 2 个功能键)
- ü LCD 显示屏能达到 10 个字母和数字混合的字符。

- ü 可替换的标准锂电池和备份电池
- ü 低电量检测特性
- ü 每个令牌有全球唯一的序列号

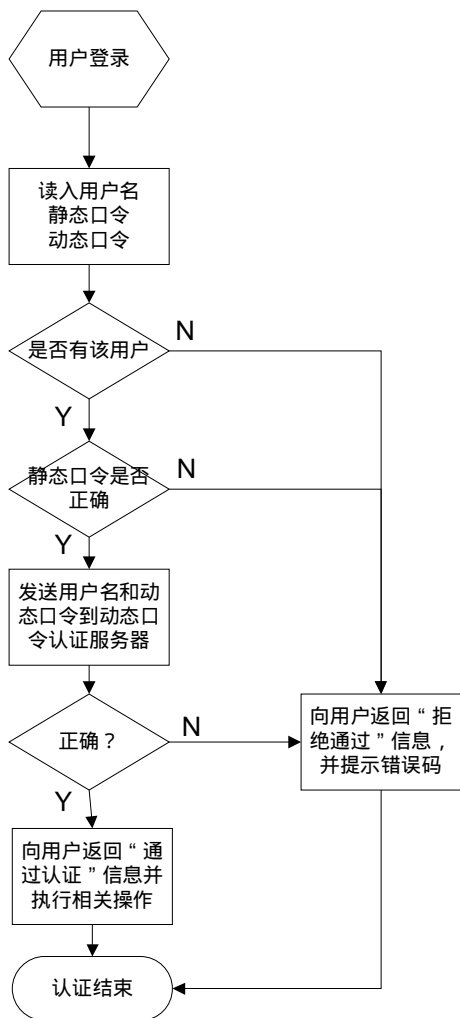
遵从的标准

- ü ANSI X3.92 数据加密(DES) 算法
- ü ANSI X9.9 动态密码计算和显示标准
- ü ANSI X9.17 DES 密钥管理
- ü ANSI X9.19 信息认证
- ü ANSI X9.24 DES 密钥导出
- ü ANSI X9.26 登录

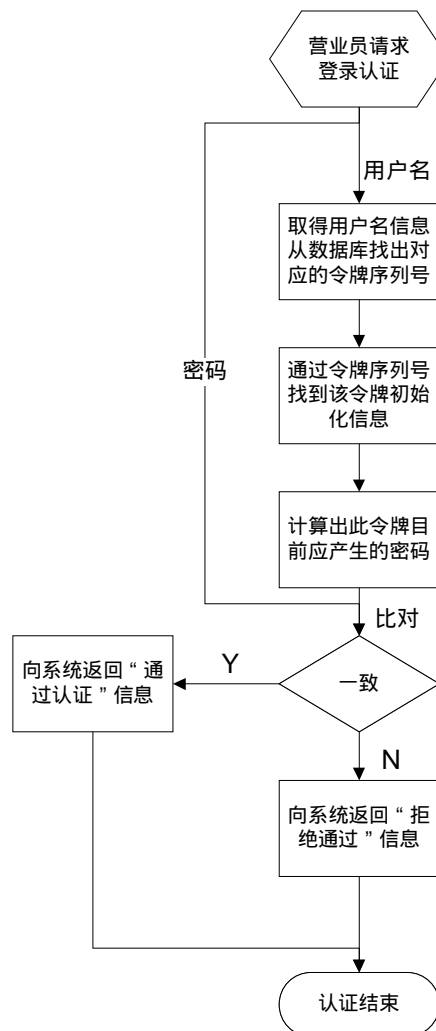
3.3 认证系统拓扑图



3.4 认证流程



动态口令认证客户端认证处理流程



动态口令认证服务器端认证处理流程

3.5 令牌发放，部署和管理

在银行的中心机房，放置一台前置机，作为令牌的管理中心，负责统一发放令牌以及令牌的新增，删除和管理工作，以及系统内各项日志的记录和审计工作。

动态口令身份认证系统前台采用 MS Windows 操作系统的服务器，在该服务器上完成令牌的管理工作。

分发和管理的主要内容包括：建立营业员管理档案数据；负责营业员的身份管理工作(新增，删除，暂停等)；负责令牌的分发和部署工作(包括发放，查询、变更、挂

失、解除发放，停用、重同步、解锁、测试等工作)。

3.6 故障/应急处理

在系统中，因为应用环境的复杂性以及使用过程中各种情况的出现，会出现一些故障或者一些需要应急处理的情况。

3.4.1 营业员无法使用令牌产生的动态密码正常登录

此种情况将会在营业员登录提示“动态密码错误”。

出现此故障，有以下两种原因：

1、 营业员看错密码，或者在登录窗口中输错密码。

-解决方法：核对密码后，在登录窗口重新输入。

2、 令牌的时间/事件参与认证服务器端失步。

-解决方法：打电话给认证系统管理员，营业员输入 PIN 码，从令牌菜单中调出相关时间/事件参数，并把相关参数值通过电话告诉管理员。管理员通过动态口令身份认证系统的“令牌重同步”操作，对令牌进行远程同步，同步操作完成后。营业员关闭令牌显示，重新开启，即可登录。营业员操作步骤详见《令牌使用手册》。

3.4.2 营业员遗忘令牌 PIN 码

如果营业员遗忘自己所持令牌的 PIN 码，并且尝试使用错误 PIN 码开启令牌超过六次(次数出厂时可选)，令牌将自动锁定。此时再次尝试开启令牌会提示“LOCKED”，并且随后只显示一个 8 位(位数可选)的“解锁挑战码”。营业员此时应该停止再次尝试。并且通过电话，把此“解锁挑战码”告诉认证系统管理员。系统管理员把该“解锁挑战码”输入到认证管理系统，得到一个“解锁应答码”，通过电话告诉营业员，营业员把管理员告知的“解锁应答码”输入到令牌后，令牌即告解锁。并且，令牌会立即提示设置新的 PIN 码。

3.4.3 令牌遗失、暂时未携带、或者发生故障

如果营业员令牌遗失正在补办过程中，或者令牌暂未携带。系统管理员可以

通过动态口令管理系统为营业员生成一个临时的(一次有效或特定时间内有效)静态密码。

当营业员使用动态口令管理系统设定的一次有效的静态密码时，系统会为该用户设定应急标志。当该营业员进认证时，应输入此一次有效的静态密码，经系统识别后确认通过认证。不管用户是否输入正确，此一次有效的静态密码都从系统中消失，无法重复使用，以此确保此静态密码一次有效。

特定时间段内有效的应答数只在指定的相应特定时间段内使用才有效。

备用令牌是管理人员为某一个营业所，或者是某几个营业员配备的备用的令牌。平时放置在营业所，在动态口令管理系统中也不被启用，当营业员正在使用中的令牌出现故障，可以随时启动备用令牌，通过动态口令管理系统进行发放，就能立即被用于故障令牌所属的营业员。

在正常情况下，ActivIdentity 令牌从发放到营业员手中，一直到令牌寿命终结为止，都无需集中收回进行维护。而可以通过远程(电话/网络)等方式，进行维护。大大节省了各项成本。

3.7 认证数据传递的安全性

动态口令身份认证系统的本身具有较强的安全性，具备防窥探、防嗅探、防穷举算法等特性，再结合景荣业务系统现有的数据安全传输机制，将更好地增强安全性和完整性！

3.8 日志和审计信息

动态口令身份认证系统提供下列几种日志和审计信息：

- 1、认证日志：记录营业员登录的用户名(用户代码)，营业网点信息，登录时间、拒绝或者通过等信息。
- 2、操作员管理日志：记录对动态口令身份认证系统本身进行操作的管理人员的所有操作日志。例如管理员登录，删除令牌，删除用户，重同步操作等等。
- 3、应急和告警日志：记录应急及故障信息。

以上信息为管理员实时监控系统的使用情况提供了多方便利，为出现安全问题时的责任、故障点分析提供了翔实的信息。

3.9 安全管理制度

通过部署动态口令身份认证系统，大大加强了金融业务系统的安全性和可靠性，杜绝的大部分内部管理安全漏洞。但是，仅仅有技术措施是远远不够的，为了便于银行更好的使用动态口令身份认证系统，启迅提供了一系列完整的管理制度，包括身份管理，令牌管理，授权管理，应急管理，档案管理等等，这些管理制度的有效执行，才能与动态口令身份认证系统无缝融合，使银行能够更快捷，更有效地部署和实施动态口令身份认证系统。

第四章 系统特点及综述

4.1 专用于银行柜员管理的安全解决方案

使用动态口令身份认证系统，利用动态口令独有的特点，可避免由于使用静态密码而造成的口令被盗用，执行权限制度不严格等安全问题和弊端。

4.2 不改变终端和网点的硬件系统

便捷的集成和实施流程，在网点端无需安装任何硬件设置，仅需要更新终端界面。

4.3 令牌无需接触式维护

在正常条件下，令牌生命周期内无需进行接触式维护，可远程进行重同步，解锁等维护操作，免除现场维护方面的成本开销。

4.4 系统稳定，技术领先

ActivIdentity 动态口令身份认证系统以可升级性强，稳定性高，集成流程迅捷等特点，能够有效地解决当前银行业务系统中的安全隐患，为实现更有效的安全性和可靠性提供技术支持和保障。

良好的设计理念，领先的技术优势，为银行在远程授权、身份验证等方面提供了强有力的技术支持能力。

4.5 令牌性能优越，总体拥有成本低

令牌使用方便，可更换电池，寿命长达 8 到 10 年。并且经过全球近千万用户多年的使用考验，故障率极低，总体拥有成本(TCO)非常低，性价比极高。

ActivIdentity 动态口令身份认证系统，必将为银行提供更高的安全体验！