



技术与解决方案

Technologies and Solutions

银行柜员系统动态口令身份认证解决方案

银行柜员系统安全现状分析

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，如冻结账户、资金转账等。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。

现有银行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。

在某些银行业务系统中，普通操作人员需要在数个营业网点之间进行轮岗，为管理方便，轮岗人员在其轮岗网点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，银行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。



技术与解决方案

Technologies and Solutions

飞天动态口令身份认证系统可以作为银行综合业务系统的内部管理子系统，为银行内部管理和银行业务管理提供安全可靠的身份认证支撑。

飞天动态口令身份认证解决方案，在现有的银行业务系统中采用动态口令进行身份认证的方式，很好地解决了现在固定口令机制的安全隐患。提供了一整套完整的解决方案来为银行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静态密码保护；令牌持有人在令牌丢失后能立即挂失；如果他人不能同时得到令牌及静态密码，也就不能冒用令牌持有人的身份进入银行业务系统；令牌产生的密码一次有效，也不用担心被人盗取。

在现有银行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静态口令和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。

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静态口令和动态口令两项认证。

首先，柜台操作员在登录窗口输入帐号、静态口令和动态口令，银行业务系统会首先验证帐号和静态密码，只有这两者通过以后，才会将动态口令发送到动态口令认证服务器进行认证并根据验证结果决定是否允许操作员登录，（图1所示）。

- (1)柜台操作员登录业务系统时，输入帐号、静态密码和动态口令；
- (2)系统首先判断输入的帐号是否存在，如果不存在，直接返回认证失败，如果存在，则继续进行认证。
- (3)银行业务系统服务器验证静态密码是否正确，如果不正确，直接返回认证失败，如果静态密码正确，则继续进行认证。
- (4)认证服务器验证动态口令是否正确，如果不正确，直接返回认证失败，如果正确，柜台操作员登录银行业务系统成功。

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

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时，可向相应授权人员申请对此项业务的权限，例如当普通操作人员需要处理冻结账户业务时。

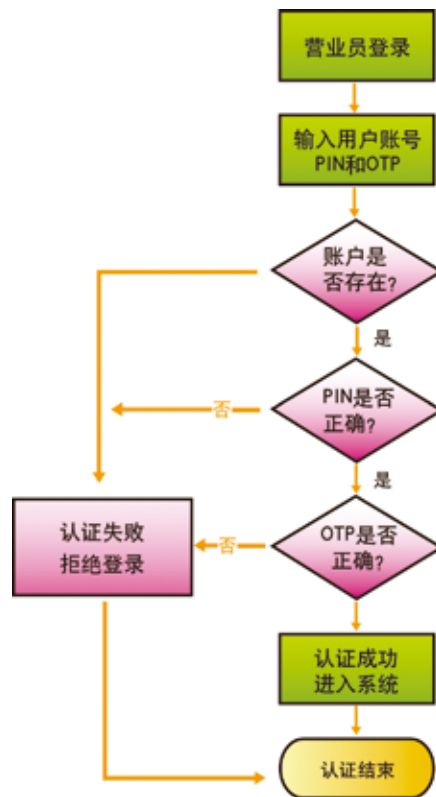


图 1 系统登录认证流程



技术与解决方案

Technologies and Solutions

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、柜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、柜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动态口令令牌生成动态口令，并把动态口令告知柜台操作人员。

柜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。

(图2所示)。

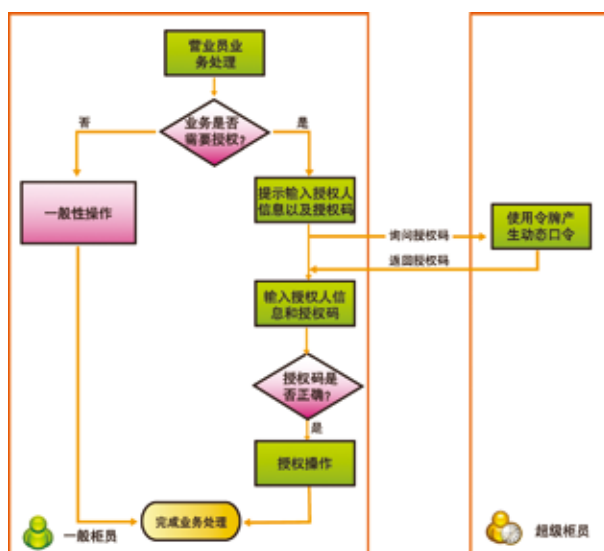


图 2 授权认证流程

上述认证流程，严格限定了业务授权的一次有效性，柜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柜台操作人员，柜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。

轮岗管理

在实施动态口令身份认证的银行业务系统中，轮岗人员的帐号和令牌可以分开管理，当轮岗人员到一个新的网点工作时，必然会为其设置一个工作帐号，此时只需要通过后台管理系统将轮岗人员以前的工作帐号与其令牌解除绑定，并将新的工作帐号与其所持有的令牌进行绑定即可，可以轻松实现轮岗不换令牌的要求。

通过部署动态口令身份认证系统，大大加强了银行柜员系统的安全性和可靠性以及操作和管理上的方便性，可以杜绝大部分内部管理安全漏洞。为了进一步提高动态口令身份认证系统的效果，银行还应制定相关的规章制度，严格对涉及动态口令身份认证系统安全的令牌管理、用户管理、应急管理等内容进行管理和控制。