

使用 ePassNG

降低网银系统客户服务成本

随着 USB Key 在网上银行、电子政务、电子商务中的应用越来越普及,许多厂家看到 USB Key 产品的市场潜力,纷纷推出自己的 USB Key 产品。目前市场上的 USB Key 产品种类繁多,良莠不齐,给各网上银行和大型系统运营商在选择产品和运营维护带来了很大的困惑。

在网上银行和大型 CA 应用中,出于供货安全保障考虑,运营商一般都会选定几家供应商。USB Key 发行到最终用户手中,不同厂商提供的 USB Key 需要安装不同的驱动程序和中间件。当最终用户需要下载驱动时就需要用户自行判断自己手上的产品对应那个驱动程序,由于网银用户计算机操作水平参差不齐,并且许多情况下银行会要求统一产品外观,最终用户很难分辨自己使用的是那个厂商提供的产品。出现这种情况,往往用户就会咨询银行的营业网点或者打 800 电话要求提供技术支持,给运营商的维护带来了巨大的工作量。据统计,在大型系统运营商的技术支持事件中,70%是由于用户安装 USB Key 驱动及配套软件不当造成的。

另外,不同厂家的 USB Key,其硬件特性各不相同,虽然目前各个 USB Key 厂家都基本上都能提供 CSP 和 PKCS#11 接口,但由于这两个 API 函数库中都有几十个功能不同的函数,各个厂家在 USB Key 中存储数据的格式各不相同,实现上述函数功能时对硬件的操作也各不相同,并且各厂家对函数出错时的处理方式和兼容性考虑的也都不一样。特别是一些新进入 USB Key 市场厂家,在正常操作的情况下基本都能实现既定的功能,但是对于一些异常情况的处理可能没有

考虑得十分完善或者没有处理经验。而实际应用调用这些接口函数以及用户在使用过程中,可能经常会出现操作失误的情况,如输入的 PIN 码为空、输入太长的 PIN 码等。系统集成商和运营商在开发应用时就需要针对不同厂家提供的不同中间件接口编写不同的代码并作大量的测试,这给系统集成商和运营商的前期开发和后期维护造成了很大的困难和隐患,增加了巨大的工作量。

可以预见以后各银行网上银行的客户量和业务量都将会非常巨大。在发行 USB Key 和网上银行运营过程中,上述问题将成为不得不面对的重大考验。

在此,飞天经过长时间的研发和测试,开发出一套适合于网上银行系统使用的,具有跨平台硬件无关的统一中间件平台——ePassNG,以支持获得入围资格厂家的不同型号 USB Key 产品,这样各家银行只要进行一次网银系统配合、调试过程,不论最终发行的是哪个厂家的硬件,客户端使用的中间件都是一套,最终用户需要下载、安装的程序也只有一份,将可大大减少网银系统上线运营后的维护成本。

ePassNG 是一套全功能的 PKI 中间件,它向上层应用软件提供 CSP 和 PKCS#11 接口以及扩展接口,支持国家商用密码管理委员会相关双证书的要求,足以满足大部分 PKI 应用的要求,向下通过可扩展的硬件封装模块支持多种 USB Key 硬件,并且可以很容易地添加对不同硬件的支持。飞天提供的 ePass2000 和 ePass3000 这两个不同芯片和型号的硬件产品都使用同一个安全中间件——ePassNG,只要 ePass2000 可以使用的应用,ePass3000 就可以使用,不会存在兼

容性问题。同样只要经过简单的定制，ePassNG 可以很容易的支持所有入围厂家的USB Key硬件。

使用ePassNG开发的应用程序，开发时无需了解未来将要使用哪些USB Key硬件，而已经开发好的应用也可以很容易加入对新硬件的支持，无须改动原有应用。选用ePassNG作为网上银行的统一中间件平台，即使未来再次对USB Key供应商及产品进行选型，也不需要网银系统进行任何改动，仅需将ePassNG客户端安装软件进行升级，就可以保证新硬件在原有网银系统中的使用。

飞天可以根据任何一家银行的需求对ePassNG中间件进行定制，以配合银行网银软件和CA系统的要求。ePassNG不仅可以运行在Win32平台上，还能运行在Linux和Mac OS平台上。使用ePassNG，最终用户不仅能够在安装Windows系统的计算机上，还可以在安装Linux系统的计算机或者安装Mac OS的苹果电脑上使用贵行的网上银行系统，可以满足众多使用非微软操作系统的用户的需求。

ePassNG的技术特点:

- 多系统支持——可运行于 Windows、Linux、MacOS
- 多平台支持——可运行于IBM兼容PC和苹果电脑
- 多硬件支持——可支持各种USB Key或智能卡及其他硬件
- 提供标准接口——支持PKCS#11和MS CAPI应用

现有PKI应用结构与基于ePassNG的PKI应用结构对比:

现有 PKI 应用结构的缺陷:

- * CA和PKI开发商必须针对不同硬件使用不同的中间件开发
- * 原有的应用很难改用新的硬件
- * 硬件厂家必须开发自己的中间件

基于 ePassNG 构架 PKI 应用结构的优点:

- * CA和PKI开发商无须了解硬件特性只需使用ePassNG中间件开发
- * ePassNG构架的应用可以使用任何符合ePassNG标准的硬件
- * 硬件厂商只要根据ePassNG标准提供TSP就可以在原有应用中使用

