

统计局网上直报身份认证方案

方案提供：北京飞天诚信科技有限公司

方案目的：

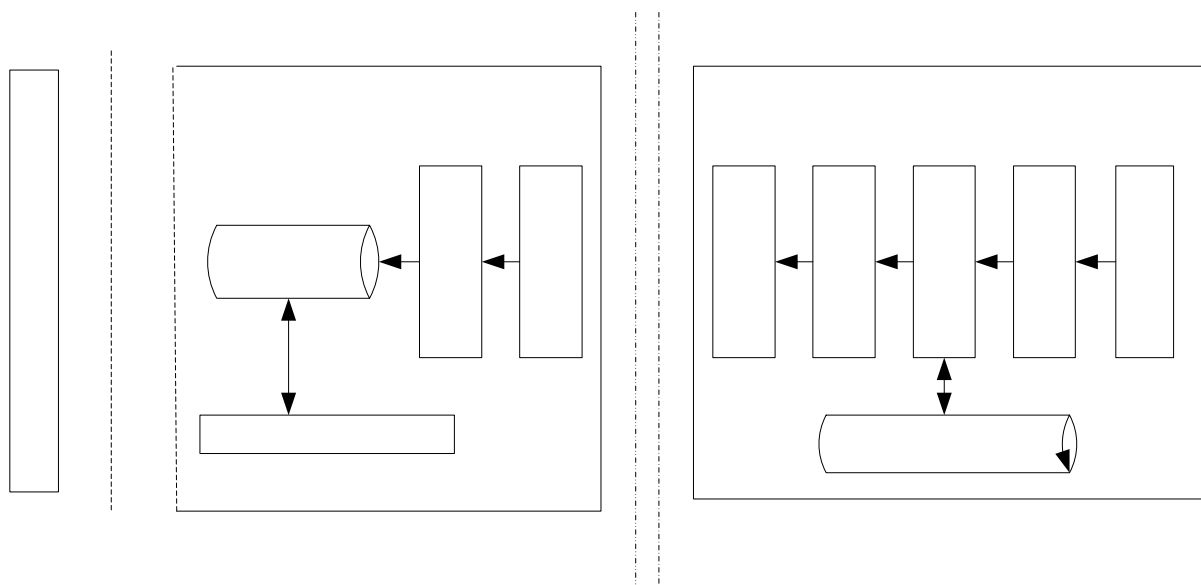
- 一、 保证统计网上直报数据的安全性
- 二、 保护企业调查对象的商业秘密

一. 项目背景

统计业务网上直报系统是利用国际互联网（Internet）完成企业用户向统计局报送月报的工作。系统采用分布式处理技术，企业和统计局之间通过 Internet 连接，采用 WEB 服务技术将企业和统计局连成一个无缝的远程系统。

在此系统中，客户端程序负责数据的用户验证、录入、审核、暂存、客户端数据备份、数据加密、数据发送的功能；服务端程序负责数据的接收、解密、入库以及用户信息管理的功能。

系统结构图如下：



二. 网上直报项目涉及到的网络安全问题

数据加密/解密技术：

数据在公用网上传输时，必须考虑到传输过程中可能出现的侦听/截获的情况。为此，数据在传输前必须经过加密处理，在服务器端进行反向解密的处理。

身份认证技术：

本系统的安全认证指的是需要保证适用本系统的企业及统计局端的操作人员具备足够的权限，以避免发生谎报、误报、数据泄漏等情况的出现。

三、我们所采用的方案

目前，网络安全以及身份认证技术，有很多种，考虑到成本以及高效实用性上我们采用了 ePass1000，一种 USB 接口的硬件认证设备。

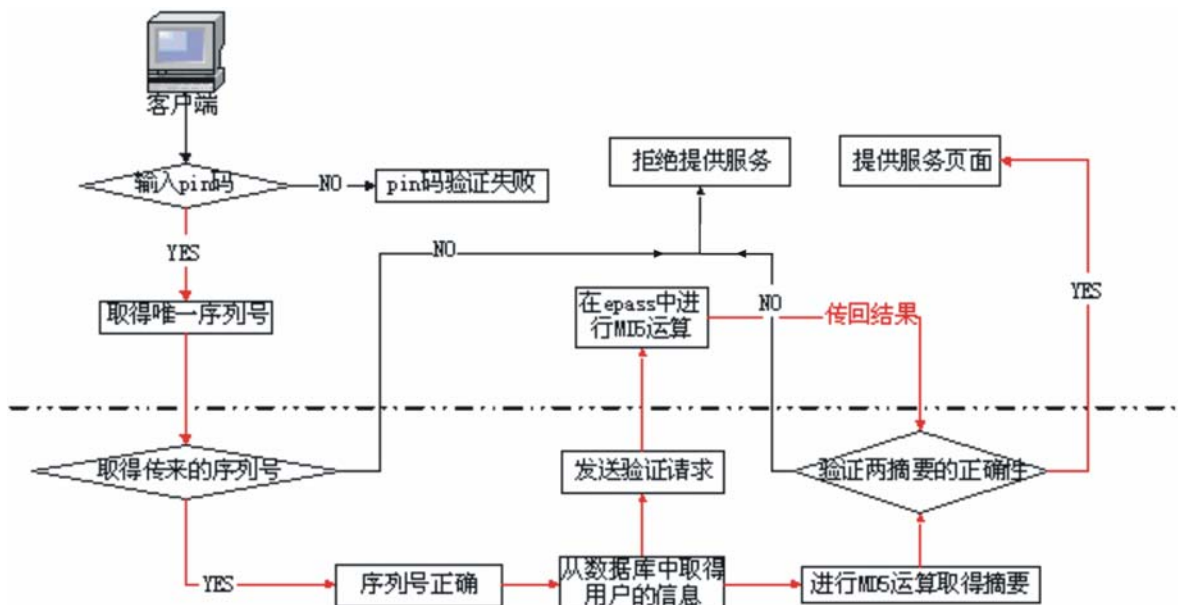
利用 ePass1000 进行身份认证：

针对于防火墙、加密技术、漏洞扫描和入侵检测技术，业界已经有很多产品方案并形成标准。因此我们在叙述我们的方案时，前提假设服务器端是安全的，即没有黑客闯入偷取数据，没有内部人员篡改数据，存储在服务器上的数据不会流失。

每当客户端有一次服务申请时，服务器先产生一个随机数给客户端，客户端的 ePass1000 用此随机数作运算的输入返一个运算结果给服务器，服务器端作相同的计算。并把计算结果与客户端上传的结果相比较，全过程可简单由以下关系式来表示：

$$ePass1000(S, K) = Server(S, K)$$

其中 S 代表由服务器提供的随机数，而 K 则代表密钥，ePass1000(S, K) 代表是插在客户端的 ePass1000 所进行的运算，Server(S, K) 代表是服务器程序的运算。而等式两端的 K 并不在客户端出现，也未直接在网上发送，这就保证了此认证方案的可行性。验证流程如下图所示：



PIN 码保护（可选部分）：用户可以利用 PIN 码来保护自己的 ePass1000，防止被别人擅自使用。操作类似信用卡，用户可先输入 PIN 码，PIN 码正确则可进行下一步操作，PIN 码错误则拒绝。

1. 取得序列号：

序列号可以是任何字符串或数字(如在数据库中的用户的账户或是 ePass1000 的硬件 ID 号)，可以是用户输入的字符串，或是从 ePass1000 中特定的文件中读出等，发送给服务器。

2. 服务器发出验证请求：

当服务器接受到客户机的序列号时，需要对序列号的真实性进行检查。因此，服务器开始对客户机的 ePass1000 进行 MD5 哈希信息码校验。要进行 MD5 校验，服务器需要传递给客户机一个随机数，并且服务器必须记住这个随机数。

3. 客户机响应服务器验证请求：

将服务器传来的随机数传给 ePass1000 并在 ePass1000 内部进行 MD5 哈希信息码运算，从而得到 128 位的摘要。这个摘要返回到服务器端。

4. 服务器判断客户机的响应：

服务器接收到客户机返回的摘要与序列号。根据序列号找到先前保存的随机数，和后台数据库中保存的用户持有的 ePass1000 的硬件 ID 号，以及 ePass1000 中 MD5 哈希信息码的内容。然后使用这些数据进行 MD5 哈希运算，得到一个 128 位的摘要。将这个摘要与客户机返回的摘要进行比较。相同则认为是合法用户，否则是非法用户。

传统身份验证方式与 ePass1000 认证方式：

身份验证在网络安全中起着举足轻重的作用，它是上网的第一步。

比较常用的身份验证方式一种是采用“密码 + 用户名”，一种是利用 IC 卡，还有一种是利用计算机的特征码(如 CPU 序列号、网卡序列号等)或者是人体特征码(如指纹、瞳孔视网膜等)来实现。其中第一种是最常用的验证机制，对安全要求较高的喜欢后两种。

“密码 + 用户名”：网络环境中，密码很容易散播、泄漏。如密码在传输过程中被截获、使用者或无意或有意的透露，造成密码很难控制。往往造成一个账户多人在使用的局面。这就损害了网站的利益以及其合法注册用户的利益。

利用 IC 卡验证：IC 卡的安全性较高，IC 卡芯片无法复制篡改以及 IC 卡技术成熟，有标准可遵循，使其在网络安全领域占有一席之地。但是如果把其应用到身份验证方面，由于 IC 卡需要专用的读取设备，成本居高不下，并且携带不便，无法大范围普及。

利用计算机的特征码验证：由于其管理复杂，灵活性较差，计算机硬件发生变化时需重新提交特征码申请授权，客户不能随便利用一台计算机登录，对于经常外出的用户就不是很方便。现在仅限于特殊的应用方面。

利用人体特征码验证：这方面比较成熟的技术是指纹识别、视网膜识别技术。但是都需要专门的读取录入设备，对最终的使用者来说成本高，读取设备不便携带。使用仅限于安全性要求极高的场合，对于商业网站是无法普及应用。

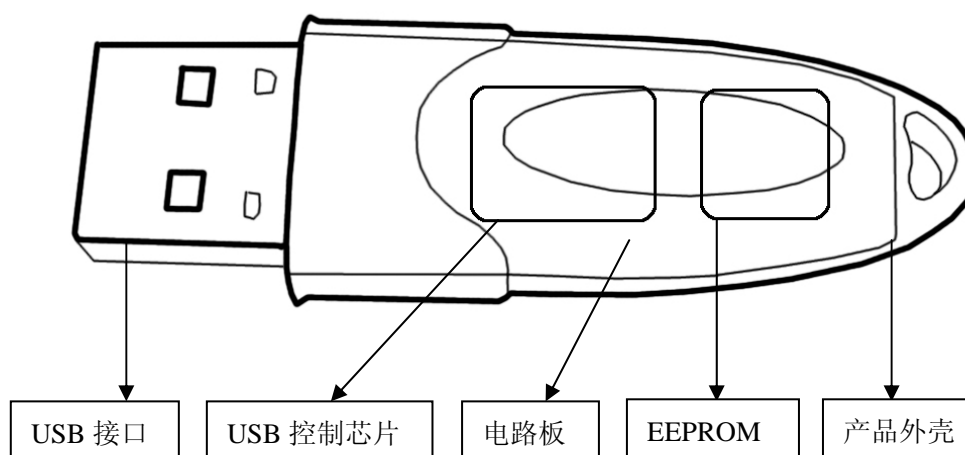
ePass1000 认证方式：由于 ePass1000 本身是一个独立小巧的数字设备，而又无需专用的读写设备。验证过程中，密钥不在网络中传播，增加了安全性。携带方便、成本较低，已经在网络中广泛使用。

ePass1000 介绍：

ePass1000 是一种低成本、便携式、通过 USB 接口与计算机相连的硬件设备。ePass1000 不需要附加电源及类似于 IC 卡读卡器设备，只有拇指般大小，可穿在钥匙链上，方便使用者随身携带。

ePass1000 适用于强双因子认证和安全存储介质。ePass1000 可以基于冲击响应体制实现对用户的强双因子认证；更广泛的应用是用作安全存储介质，存取重要信息。如，把数字证书、私钥、密码、信用卡号、或其它安全认证信息，如果都存放于 ePass1000 中，并带在您的身边，将更加方便、更加安全。

(一)、ePass1000 硬件结构



主要物理构件包括：USB 控制芯片、EEPROM（电可擦写可编程只读存储器）、电路板、USB 接头、产品外壳。

1. USB 控制芯片采用专用 USB 通讯芯片，用来处理计算机向 ePass1000 传来的各种命令，以及完成对存储在 EEPROM 中的信息进行加/解密和完成硬件的 MD5-HMAC 算法。
2. EEPROM(电可擦写可编程只读存储器)主要是完成存储信息的功能，如存储证书、公钥、私钥或文件，目前的存储空间有 8K、32K 两种。
3. 电路板主要完成的功能是将电路板上的各个芯片进行连接，实现芯片之间通讯。
4. USB 接头主要完成的功能是将计算机与电路板进行联接，实现计算机与 ePass1000 的通讯。
5. 产品外壳主要实现的功能是对内部部件的保护，同时还具有美观的功能。
6. 电路板、USB 接头、产品外壳相应的供应厂家都通过了 ISO9002 系列质量认证或国际 UL 质量认证。

(二)、安全体系

1. 逻辑防护措施

1. ePass1000 只允许单进程访问，确保不被跟踪。
2. 设有两层目录结构，通过文件系统保证数据文件的安全。

3. 文件系统受三层密码体制保护，通过密码设备对使用人员的身份合法性进行认证。没有 PIN 码、管理员密码无法访问某些文件。即使知道密码，如果不掌握文件的数据结构也无法获得私钥。
4. 设置 PIN 码的最大可重试次数。当 PIN 码连续输入错误达到最大可重试次数时，ePass1000 自动锁死，这样就成功的防范了穷举攻击方式，当 PIN 码被锁死时，管理员需要重新进行解锁。
5. 针对强双因子认证模式，密钥的生成和运算都是在 ePass1000 内部进行的，外部无法使用软件跟踪算法。
6. 密钥文件属性为不可读，无法获得密钥。算法采用的是值得信赖的 MD5 HMAC 算法。这样，算法、密钥、运算三个因素都是安全的，也就确保了整个认证过程的安全。

2. 硬件防护措施

CPU 与 EEPROM 一一对应，即使将两个 ePass1000 中的 EEPROM 进行互换，也不可以获得另一个的信息。

ePass1000 采用一体化封装的外壳，防水、防尘、防震。如果以物理方式打开 ePass1000，里面的物理结构将遭到破坏，确保存储信息的机密。

3. 文件系统

ePass1000 在硬件层提供了三种安全状态，超级用户、普通用户、匿名用户。

超级用户 (Security Officer) 状态

超级用户是拥有最高权限的用户状态。超级用户需要一个 PIN 码。在这种状态下允许对硬件的许多重要的参数设置及 ePass1000 的初始化，并且一旦忘记了此密码，就无法再以此身份操作 ePass1000 了。此时只有送回厂商，对其重新烧制，但原有的数据将全部丢失。

普通用户状态

在此状态也会提供一个用户密码，而且允许用户去修改密码。存储于 ePass1000 中的个人信息也是在此状态下进行访问的。同时在硬件层实现了一个登录密码计数机制，每当提供的密码不正确时，计数便会减少，而登录成功时计数便会重置为最大值。当此计数减至零时，ePass1000 便会处于锁定的状态。此时只有超级用户（管理员）才能将此记数值重置，解除锁定的状态。

匿名状态

匿名状态是 ePass1000 的缺省操作。匿名状态允许有限的对公开信息的读取操作。

文件类型

ePass1000 文件系统使用两种类型的文件：

类 型	描 述
数据 (DATA)	任何变长的二进制的的数据
密钥 (KEY)	用于加密的数据

文件存取控制

ePass1000 的文件有三种存取控制类型，每个文件有它自己的存取类型控制设置

存取控制	文件类型	
	数据 (Data)	密钥 (KEY)
读	由属性决定	禁止
写	由属性决定	由属性决定
加密	无意义	由属性决定

注意：读写操作是 ePass1000 的数据传输的功能。加密对于数据 (Data) 类型的文件来说是无意义的。对密钥 (KEY) 文件的加密操作完全在 ePass1000 的内部完成。

文件访问权限

属 性	Description
ALWAYS	总是允许访问
NEVER	从不允许访问
PIN	在普通用户及超级用户状态可访问
SO PIN	仅在超级用户状态可访问

注意：多个应用程序使用同一个 ePass1000 硬件时，应根据情况相应调整其所使用的目录或文件 ID 以免冲突。

根据我公司多年的经验积累和一些项目运作经验，一个项目要成功除了要具备良好的商业模式、先进可靠的软硬件平台，还要考虑市场需求，即最终消费者对产品、服务的接受程度。

便利性

ePass1000 不需要附加电源及类似于 IC 卡读卡器设备，只有拇指般大小，可穿在钥匙链上，方便使用者随身携带。

通用性

ePass1000 是通过 USB 接口与计算机相连的硬件设备，适合当今国内绝大多数计算机操作环境；提供多种的驱动程序，消费者可以在各种主流操作系统上应用。

适用性

ePass1000 价格低廉，可以满足消费者大多数应用需求，性能价格比极佳，适用性极强。

个性化

ePass1000 提供多种形状外壳，配以多种时尚的颜色，满足消费者个性化的需求。

兼容性

ePass1000 不仅提供私有接口，同时还支持 MS CSP、PKCS#11 标准，提供完整可靠的中间件，满足各种应用平台。

(飞天诚信公司 www.FTsafe.com)

ePass1000 硬件电器参数

操作系统	Windows 98/ME/ 2000/XP/2003, Mac OS 8/9/10.x, Linux
证书及标准	PKCS#11, MS CAPI, PC/SC, X.509 v3 证书存储, SSL, IPSec/IKE
内存容量	8K、32K
硬件算法	MD5
芯片安全级别	安全加密数据存储
外形尺寸	58 x 14 x 7 mm 或 50 x 17 x 7 mm
重量	8g 或 6g
功率	< 250 Mw
工作温度	0°C至 70°C
存放温度	-40°C至 85°C
湿度	0 至 100%, 不结露
接口类型	USB A 型 (通用串行主线)
封装	硬塑料防篡改
数据保存年限	至少 10 年
内存写次数	至少 10 万次