

## EPass 身份认证锁在气象预报系统中的应用

### 背景需求：

一直以来，专业气象台为一些行业用户（例如：电力、交通、农业等系统）提供专业的气象服务，都是通过电话、传真形式来完成的。由于每天需要有专人逐个用户通知，工作量非常大，效率低而且及时性较差。越来越无法满足人们方便快捷的要求。随着互联网的普及，通过互联网站发布天气预报，由于成本低（节省人力），方便快捷（随时可以查询），跨地域性（任何上网的地方都可以）等诸多优点，受到各地气象台的喜爱。但是，天气预报作为国家控制的资源信息，并不是对所有的人开放的。而且有些分析数据是针对一些专业的用户而设计的。因此，系统必须有身份认证与鉴权机制。

系统设计之初没有太多安全方面的考虑，只是简单地发给用户一套“用户名和密码”，让用户凭此进入系统。后来偶然间发现，有些用户的账号同时在 2 个不同的地域登陆到系统中来，用户帐号密码共享（/被盗）！为此需要重新更改身份认证方式。提高系统安全性，保护用户的利益。

目前身份认证的手段有多种多样，例如：“用户名+密码”认证、IC 卡认证、生物识别技术、动态口令卡/牌、USB TOKEN、数字证书人证等，而且各有优缺点。系统设计之初，就确立了安全性高、使用方便、低成本、开发难度低、携带方便、小巧（如果有硬件）等基本要求。

### 几种身份认证方式的介绍：

1、密码+用户名——作为一种低成本、方便的使用形式，此种方式在网络应用中很普遍。但是由于“密码”和“用户名（或者账号）”作为软性标识，很容易忘记或者被他人有意或无意获取。因此只是适合一些安全性要求不高，即使丢失被他人使用或盗用也不会产生巨大影响的应用中。

2、动态口令卡（令牌）——这是一种新型的密码认证的改进型。是为了弥补“密码+用户名”认证中，静态口令如果设置复杂不容易记忆以及容易被别人获取的缺陷。认证中用户口令是动态改变的，一般会发给用户一个令牌，上面显示的数字是随时间变化的。这串变化的数字就是用户进入系统的口令。该系统由用户端的密码卡和应用系统端的认证服务器组成。用户登录应用系统时，依据安全算法，认证系统会在密码卡的专用芯片和认证服务器上同时生成动态密码，经过比较，若双方密码相同，则为合法用户，否则为非法用户。

用户端的密码卡使用起来非常简单。用户登录前，只要在卡上输入由用户掌握的开启 PIN 码，卡上就会显示出当前生成的动态密码，用户按照此密码登录即可。

动态口令卡解决了服务器端认证用户端的身份认证，但是不能反向认证即用户端认证服务器端身份。同时有一个时间同步的问题，如果用户端与服务器端之间时差很大或者网络速度较慢，客户就会因为网络延迟而无法登录到服务器。

3、生物识别技术——是利用人们的生物特征（如指纹、声音、视网膜等）来进行识别的一种高安全的解决方案。此技术是预先收集目标用户的生物特征样本，存储在系统中。用户在使用时，只是进行简单地操作（如把手指放在指纹扫描器上），系统采集到活体数据与存有的样本进行比较，以此来完成身份的判别。但是由于人体生物特征的采集与整理需要昂贵的设备。对于网络应用中，如每一个用户端安装一个数据采集装置，成本是一个瓶颈。如若再考虑移动上网的用户，此种认证方式并不适合。因此目前仅适用于安全性较高的固定场合，如银行、门禁等。

4、智能卡身份识别技术——智能卡作为一种身份识别技术开始于九十年代。互联网发展以来，许多厂家把 IC 卡作为身份认证的解决方案提供给用户。但是大批量使用 IC 卡时人们遇到了困难——IC 卡片与读卡器的总体成本较高；读卡器体积庞大不便于携带；各种读卡器的标准不统一，任何一种读卡器都无法读取市面上所有的 IC 卡片。

5、USB TOKEN (/KEY) 身份认证——这是一种新兴的认证设备。他是结合 IC 卡技术、读卡器技术、USB 技术为一身的认证设备。他不仅支持挑战握手认证协议 (Challenge Handshake Authentication Protocol CHAP)，同时还可以当作数字证书的存储介质，结合安全中间件，利用数字证书完成身份认证。它采用 USB 接口与计算机相连，外观小巧、携带方便。由于采用 IC 芯片安全性较高。

6、基于 PKI 体系的数字证书认证——数字证书就是网络通讯中标志通讯各方身份信息的一系列数据，提供了一种在 Internet 上验证您身份的方式，其作用类似于司机的驾驶执照或日常生活中的身份证。它是由一个权威机构——CA 机构，又称为证书授权 (Certificate Authority) 中心发行的，人们可以在网络交往中用它来识别对方的身份。数字证书不仅能进行身份认证，同时数字证书还能确保信息传输的保密性、数据交换的完整性、发送信息的不可否认性。但是由于 CA 系统实施复杂，项目庞大并且维护成本高。无法用在中小型应用中。

在几种认证方式中，USB TOKEN 认证技术简单、集成开发工作量小、成本低、使用携带、安全性较高，满足系统要求。因此决定在系统中采用。

技术实现：

北京飞天诚信科技有限公司作为国内最早生产自主知识产权 USB TOKEN 的厂家，其身份认证产品——ePass 身份认证锁在业界享有很高的知名度。其中 ePass1000 能满足系统要求。

## 强双因子认证



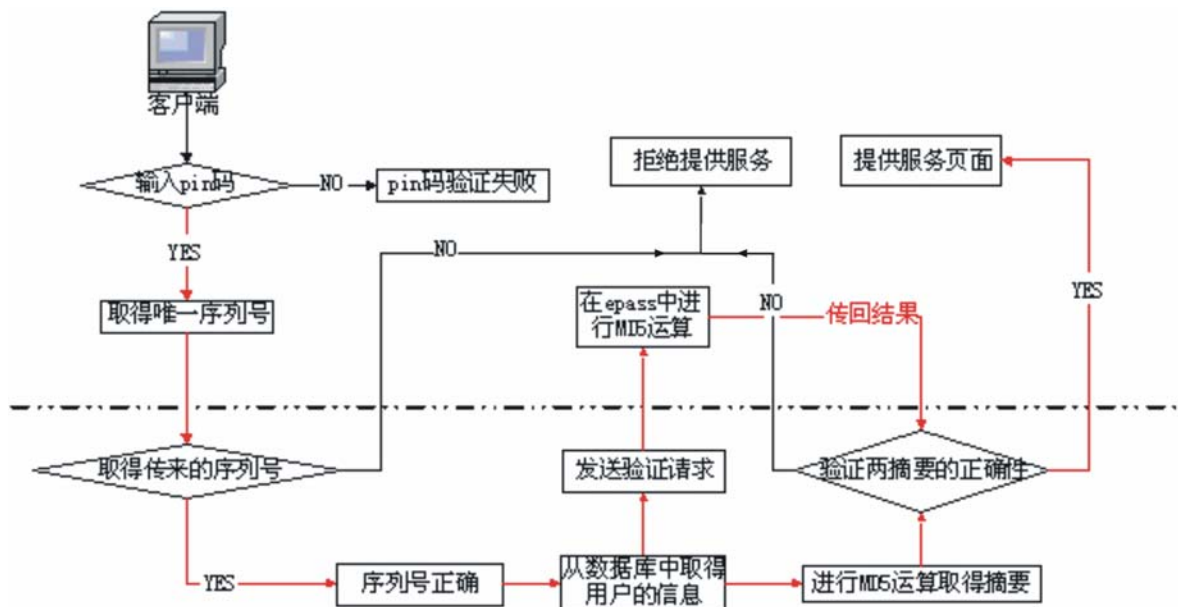
ePass1000 支持强双因子认证意味着不仅仅要有硬件，同时还需要硬件的 PIN 码才能使用完成认证工作。下图为 ePass1000 基于冲击响应体制实现强双因子认证流程示意图以及 ePass1000 在网络安全登录拓扑图：

在整个认证过程中，ePass 采用冲击响应的认证方式，利用 ePass 内置的随机查询数生成器，当需要在网络上验证用户身份时：

- 1、先由客户端向服务器发出一个验证请求。
- 2、服务器接到此请求后生成一个随机数并通过网络传输给客户端（此为冲击）。
- 3、客户端将收到的随机数提供给 ePass，由 ePass 使用该随机数与存储在 ePass 中的密钥进行 MD5-HMAC 运算并得到一个结果作为认证证据传给服务器（此为响应）。
- 4、与此同时，服务器也使用该随机数与存储在服务器数据库中的该客户密钥进行 MD5-HMAC 运算，如果服务器的运算结果与客户端传回的响应结果相同，则认为客户端

是一个合法用户。

认证流程如下：（虚线下面是客户端的操作，虚线以上是服务器端的操作）



## EPass1000 的安全性

1. ePass1000 只允许单进程访问，确保不被跟踪。
2. 导致每次登陆认证过程中认证服务器与客户端之间的数据往来每次都不相同。如果黑客简单截获到认证过程的数据仍无法在网络中冒充 ePass1000 客户端。
3. 设有两层目录结构，通过文件系统保证数据文件的安全。
4. 客户密钥是存在于 ePass1000 中，作为一种特殊的文件存在（KEY 文件），本身是不可读，而且可以设置用 PIN 码保护。
5. 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。
6. 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。
7. 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。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。

应用环境：

客户端：

- 1、浏览器（IE、Netscape 等）——操作系统自带或免费下载
- 2、驱动程序——硬件产品驱动程序，厂家提供
- 3、控件或插件——驱动程序中自带，也可以自行开发
- 4、PIN 码更改程序——应用开发商开发（厂家可以提供），可放到网页中

服务器端：以下需要应用开发商进行开发。

- 1、用户数据库——记录用户信息、密钥以及其他信息
- 2、认证服务程序——提供认证服务，实现 MD5-HASH 运算以及数据校验
- 3、发卡、注销管理程序——连接到用户数据库，进行发卡初始化工作，并且可以对用户的权限进行设置

应用效果：

系统完成两年多来，用户使用良好。从气象台而言，目前使用 ePass 做网络身份认证的专业气象台都能有效的控制会员的管理，解决了以前以账号形式分发给用户造成一个帐号多人使用的局面。对于会员的登录管理、服务管理、账号管理都能有效控制和解决，从最大程度上保证了专业气象台的利益，并形成了良好的专业气象服务意识和一定的商业模式。

在客户方面，以往采取年或月的收费方式来进行气象会员的收费。用户交了钱得到了一个账号和一个密码，感觉没有硬件的实体和身份的尊重。现在 ePass 能够打消他们这方面的顾虑。给客户一支灵巧精美的 USB key，并且可随身携带，持有 key 的 VIP 会员和没有 key 的普通会员在进入网站首页时看到的就不一样了，有 key 的会员插入 key 以后能看到专门的 VIP 登录窗口，而普通用户是绝对看不到的，这样可让客户尽显尊贵身份的同时又提高了我们网站的安全系数！让黑客或恶意份子的攻击无从下手！真正做到安全认证！

典型用户：

贵州气象台

重庆专业气象台

成都专业气象台