深圳市海月通信技术有限公司

证卷行业动态密码解决方案

建议书

深圳市海月通信技术有限公司

目录

1. 方案背景

在随着计算机在各行各业的广泛应用，计算机对于人们的工作和生活变得越来越重要，而很多企业正常开展工作对电脑有着严重的依赖。现代科技技术改变和提高企业的生产效率的同时，也给人们留下了信息安全的隐患，虽然各种各样的软、硬件加密技术及机制应运而生，用来保障数据在传输、处理和贮存中的安全，而守护这一“坚固保垒”合法入口的却往往是瘦弱的“用户名”和“用户密码”。因此这也成为非法进入计算机系统的重要“战场”之一，利用木马程序、网络监听、暴力破解等方式进行，都将严重威胁系统信息的安全，也成为阻碍金融、证券在网上应用的发展的一个因素。根据美国某专业安全协会对近千名公司网络管理员的调查表明，有 60%的系统首先被攻击和突破的地方是密码。

网上流传的各种密码截取软件、账户破解软件多如牛毛，在 Google 上搜索关键字“密码截取软件”，共搜出 128000 条记录；搜索关键字“穷举法破解密码软件”也搜出了 52400 条记录。

除了可能会被黑客软件等盗取外，静态密码还很明显存在如下的安全隐患：

1）用户在输入密码时容易被人偷看或者摄像机记录；

2）用户的密码一般有一定的规律性，容易被猜测；

3）用户的密码长期不变，容易泄漏；

4）内部的防范意识不强，内部员工的恶意操作；

5）因为工作需要，告诉同事密码，事后忘记修改；

密码是信息系统安全要求最高的地方，万一发生密码被盗，特别是如单位的领导，财务等一些重要的用户密码被盗，可能造成的损失将是非常巨大的，甚至是致命的。

为解决静态密码所存在的各种问题，深圳海月通信公司研发了“易安全动态密码认证系统”。用户持有动态密码卡（也叫动态口令卡、令牌），并且只有自己知道 PIN 码；密码卡每一分钟都产生一个新的密码，不可预测，并只能使用一次；密钥存放在服务器和动态密码卡中，不在网络中传输。所以，动态密码不怕被人偷看，不怕“黑客”网络窃听，不怕“重放攻击”，不能猜测，不易破解，具有很高的安全性和使用方便性。

2. 动态密码解决方案介绍

2.1. 动态密码系统介绍

现有系统的密码大部分是记忆在人的大脑中，长期固定不变，每次登录的密码都一样，称为静态密码。动态密码不需要记忆，通过一个独立的手持设备产生，该设备每次生成的密码随时间变化，每次的密码都不相同，每个密码只能用一次。这样即使动态密码被盗，也不会对系统的安全产生影响，通过其特性，动态密码能够有效地保证用户的安全登录。

2.1.1. 动态密码的原理

海月通信公司的动态密码采用了基于时间、事件和密钥三变量而产生的一次性密码代替传统的静态密码。每个动态密码卡都有一个唯一的密钥，该密钥同时存放在服务器端，每次认证时动态密码卡与服务器分别根据同样的密钥，同样的随机参数（时间、事件）和同样的算法计算了认证的动态密码，从而确保密码的一致性，从而实现了用户的认证。因每次认证时的随机参数不同，所以每次产生的动态密码也不同。每次计算时参数的随机性保证了每次密码的不可预测性，从而在最基本的密码认证这一环节保证了系统的安全性。

2.1.2. 动态密码系统的工作流程

系统向每一位用户发放一个动态密码卡，用户每次将卡上当前显示的数字作为本次登录系统的密码通过计算机的键盘输入系统，即可完成登录。具体工作流程如下：

1) 用户准备登录系统；
2) 用户输入用户名称；
3) 用户取出动态密码卡，按下开机按键，输入 PIN 码，卡上的液晶屏显示一串随机密码（小卡主要通过软 PIN 码保护）；
4) 用户将随机密码通过客户端键盘输入。
5) 用户输入的所有信息被传送到后台服务器，后台服务器将用户 ID、密码传送到动态密码认证服务器。
6) 动态密码认证服务器根据客户 ID 从用户数据库中调出该用户的加密信息，将加密

信息解密得到原始信息；

7） 动态密码认证服务器使用与动态密码卡同样的加密算法对用户密码进行验证，并将验证结果返回给后台应用服务器；

8） 后台应用服务器将验证结果返回给用户，并根据验证结果赋予用户相应的权限，一次认证过程结束。

2.1.3. 易安全动态密码认证系统的构成

易安全动态密码认证系统主要由 2 部分组成，分别是：客户端(动态密码卡)，动态密码认证服务器软件。

1）动态密码卡

动态密码卡由最终用户使用，通过该卡可以生成登录需要的动态密码，为防止其它人盗用密码卡，在使用该卡前，还需要输入开机密码，这样多重保证用户密码的安全。

1）KingKey

KingKey 图

外形尺寸	50mm ×25mm × 9mm（和钥匙差不多）
电源	＋3V
随机密码长度	6 位
随机密码有效期	一次性使用
时间偏差	小于 2 分钟/年。
卡的寿命	3 年以上
其他	产品非常结实，可以经得起开水煮、洗衣机、冰雪冻、50 公斤的压力压

2）SecureKey

图 钥匙型动态密码卡

外形尺寸	50mm ×25mm × 10mm（和 U 盘差不多）
电源	＋3V
随机密码长度	8 位
随机密码有效期	一次性使用
时间偏差	小于 2 分钟/年。
卡的寿命	3 年以上

3）SecureCard

图 动态密码卡图

动态密码卡的参数：

外形尺寸	80mm × 50mm × 4.5mm（和银行卡差不多）
电源	＋3V
随机密码长度	8 位

随机密码有效期	一次性使用
时间偏差	小于 2 分钟/年。
卡的寿命	5 年以上

2）认证服务器

认证服务器部署在后台，主要包括一个后台管理程序与数据库，主要的作用是认证用户提交的动态密码的有效性，及进行一些常规的管理。主要功能包括：

1. 导入 SN，导入供应商提供的密码卡的 SN 号，包含了购买的密码卡的信息；
2. 删除 SN，删除导入密码卡的信息；
3. 用户组管理,对用户进行分组管理，用户组可以新增、修改、删除；
4. 导入用户，导入指定格式的用户到系统；
5. 增加用户，指的新开通一个用户，这里指的用户是需要登录客户应用软件系统的用户，并非登录本软件的用户。用户应用软件的用户想通过动态密码管理，必须增加这个用户后，才能使用；
6. 邦定 SN，把用户与一个 SN 号进行邦定；
7. 取消邦定,把用户与邦定的 SN 进行取消；
8. 停用，当用户的密码卡丢失后，可以通过停用处理，让用户的密码卡暂时不能使用；
9. 恢复，把已经挂失的密码卡恢复到可以使用状态；
10. 删除，把已经开通使用安全密码的用户进行删除，使该用户不可登录客户的应用软件系统；
11. 换卡，主要是把用户当前使用的密码卡更换成另外一个密码卡；
12. 解 PIN 码，当用户使用密码卡时，连续 6 次输入错误的 PIN 时，密码卡会被锁定，此时可以通过此功能来进行解琐；
13. 同步服务器密码，当用户连续生成 19～21 个(或者更多)密码，而不登录客户应用软件的时候，这时密码卡再生成的密码不可用。密码卡需要与服务器进行同步后才能正常使用；
14. 管理员操作日志，查看管理员操作系统的日志，系统记录的操作内容包括：新增

用户、挂失用户，恢复挂失用户、修改用户信息、注销用户，以及换卡操作；

15. 用户登录日志分析，可以统计分析某一时间段内用户成功或错误登录系统的数据。同时可以对应用安全策略的用户解除禁止登录系统的限制；

安全策略，安全策略是设置用户登录系统尝试次数达到规定次数时，系统中止用户与系统之间的会话。防止用户受到恶意攻击。

认证服务器特点：

1. 认证服务器支持简体中文、繁体中文、英文管理界面；
2. 软件接口提供 C /C++、java、ASP、JSP、PHP 等；
3. 生成一次性密码，密码使用后立即失效，不能重复使用；
4. 用户输入错误密码一定次数（可配置）即被禁用，在一定的时间偏移范围内允许输入下一个连续令牌码进行验证，并修正时钟偏移，达到安全性和容错性的有效平衡；
5. 服务器支持“动态密码”、“静态密码＋动态密码”的认证方式；
6. 认证速度可达到 5000 用户/秒；
7. 用户数支持大于 50 万用户数，并且可扩展；
8. 可以按指定格式导入用户；
9. 服务器可以与金蝶、用友、蓝凌等公司的软件系统结合，不需要做额外的接口；
10. 服务器可以与其它系统相结合使用；
11. **是金蝶、用友、蓝凌、沟通科技、华为、华三（华为-COM）等公司在其软件系统中唯一默认支持的动态密码认证系统；**

2.2. 证卷行业动态密码集成技术方案

深圳海月提供两种集成解决方案：紧耦合集成方案与松耦合集成方案。

紧耦合集成方案是深圳海月提供令牌认证的开发工具包和相应的 API 接口函数，证卷系统通过调用这些 API 实现用户身份的认证。

松耦合集成方案指的是深圳海月提供整套令牌后台认证系统（后台认证系统也可以通过使用深圳海月提供 API 接口，证卷公司自行研发），其中包括应用、操作系统、数据库

以及硬件平台，有些可能需要额外的中间件，令牌后台认证系统提供对外接口协议与证卷公司的系统进行互联，实现令牌的认证，一般上，松耦合的接口方式主要采用 TCP/IP 的接口方式。

2.2.1. 紧耦合集成方案

2.2.1.1.接口方式

深圳海月通过提供 DLL 文件(windows 环境)和 SO 文件(linux 环境)，提供相应的 API 函数接口，把 TOKEN 系统完全集成在证卷公司的系统中。

深圳海月主要提供：

- ✓ 密码验证接口
- ✓ 时钟同步接口

2.2.1.2.海量并发处理

由于证卷公司用户数量庞大，特别是在热点登录时间，很容易引起海量并发用户认证需求。

在紧耦合集成方式下，用户动态口令认证过程和原来静态口令认证过程很接近。因此海量并发处理的方式也将是采用目前用户认证时的负载均衡方式进行处理。

2.2.1.3.数据存放方式

紧耦合方式下，深圳海月主要提供验证、同步相关的函数库，TOKEN 卡的相关数据信息保存方式，主要由证卷公司结合现有的系统，根据具体的需求进行保存。每次调用深圳海月的 API 函数时，参数中需要传入 TOKEN 的信息，验证结束后，API 函数会返回新的信息，必须用新的 TOKEN 信息替换旧的 TOKEN 信息，以供下次使用。例如：

动态密码验证函数原型： int TokenPasswordCheck(char *cInitTokenInfo, char *cPassword, char *cReturnTokenInfo);

当用户验证时，需要传卡的初始信息 cInitTokenInfo 进来，验证结束后，函数会通过参数 cReturnTokenInfo 返回验证后的 TOKEN 信息。应用系统需要使用返回的

cReturnTokenInfo 替换初始的 cInitTokenInfo，下次调用时，使用上次返回的 cReturnTokenInfo 作为函数的初始信息 cInitTokenInfo。

在紧耦合集成方式下，cInitTokenInfo 信息就由应用系统进行保存。应用系统还需要考虑这些 TOKEN 信息的备份等容灾措施。

2.2.1.4.容灾处理方案

在紧耦合方式下，深圳海月主要提供嵌入式文件（dll 文件或 so 文件）的形式，直接嵌入到证卷公司的系统中。在这种情况下，TOKEN 系统和证卷公司现有的认证机制已经是完全融合成一个整体,因此容灾处理也只需和证卷现有认证系统的容灾处理一样的处理机制即可。

2.2.2. 松耦合集成方案

2.2.2.1.接口方式

在松耦合集成方案中，深圳海月将主要通过提供接口协议的方式，使用 TCP/IP 的方式和证卷公司的系统进行对接。和紧耦合类似，接口提供的功能主要是：

- ✓ 密码验证接口
- ✓ 时钟同步接口

2.2.2.2.海量并发认证方案

由于证卷公司用户数量庞大，特别是在热点登录时间，很容易引起海量并发用户认证需求。深圳海月建议采用【并列 TOKEN 认证服务器】的形式，每台认证服务器配置两台以上数据存储服务器，并且在认证服务器中，采用【内存数据库】方案解决以提高认证过程的效率。

- ✓ 【并列 TOKEN 认证服务器】：由于每个 TOKEN 有一个唯一的序列号，因此可以按照 TOKEN 序列号分段的形式，把认证负载均衡到各认证服务器中。例如：按照每 10 万个 TOKEN 设定一台 TOKEN 认证服务器，TOKEN 的序列号在 10 万段的在第一台认证，在 10～20 万段的在第二台认证，如此类推。当使用 TOKEN 的用户进行

认证时，通过查询该用户绑定的 TOKEN 的序列号，迅速负载均衡到相应的 TOKEN 认证服务器。这样就可以从负载均衡的角度解决海量并发认证了。

- ✓ 【内存数据库】：为了更好的提高处理的效率，采用通信系统中经常使用到的【内存数据库】。即平时使用的 TOKEN 数据，全部存储在 TOKEN 认证服务器的内存里面。当用户有 TOKEN 认证请求过来时，只需要在内存数据库中操作即可。由于内存数据库的所有数据全部放在内存里面，处理起来的效率要比放在硬盘等存储设备上要快得多。内存数据库的数据再通过定期备份到存储设备上，以防断电情况下数据不会丢失。使用内存数据库后，当系统第一次启动时，需要从存储设备上的数据库一次性读取全部信息，复制到内存数据库中存放。系统正常运行时，所有数据处理均在内存数据库中进行。内存数据库通过定时器的方式定期备份数据存储到存储设备上。

2.2.2.3.数据存放方式

如上小节所介绍，每台 TOKEN 认证服务器配置两台以上存储设备。运行中的数据主要存储在内存数据库中，备份的信息则存储在存储设备上。

2.2.2.4.容灾处理方案

为了完全确保系统的安全运行性，必须考虑容灾处理。这里主要从以下几个角度考虑：

- ✓ TOKEN 认证服务器的双机热备
- ✓ 存储设备的双机热备
- ✓ 认证服务器网络的热备

针对每个 TOKEN 认证服务器，必须考虑主服务器和备用服务器的形式，当主服务器出现故障后，马上自动切换到备用服务器上。这样业务就不会发生中断。

针对每台 TOKEN 认证服务器所使用的存储设备，也必须考虑双机热备问题。存储设备的热备，建议采用现有成熟的存储设备方案，例如 IBM、EMC、华三等公司提供的存储方案。

认证服务器所使用的网络也需要考虑备份问题，认证服务器所连接的网络本身应该有容灾处理的能力。这部分建议采用证卷公司目前所使用的方案。

3. 部分成功案例介绍

3.1. 海南电信

海南电信商务领航项目中，为了增强用户身份认证的安全性，给用户配置了深圳海月公司的动态口令卡产品。目前，已有 2 万商务领航用户在使用深圳海月的动态口令产品进行身份认证。

3.2. 辽宁阜新商业银行

辽宁阜新商业银行是地方性商业银行，为了防范金融领域的信息泄露风险，阜新商行在员工登录内部业务系统中，采用了动态口令的身份认证方式。阜新商行下一步计划是把动态口令的技术应用到个人的网上银行上来。

3.3. 联合购买网

联合购买网（骏网）是全球华文最大的数字化商品销售门户，每个月销售 1 亿以上的网游点卡等数字化产品。为了彻底解决木马盗号和钓鱼网站等威胁，联合购买网采取了深圳海月提供的动态口令解决方案，目前联合购买网的用户以及经销商等均采用动态口令进行强身份认证。

3.4. 金蝶软件

金蝶软件是深圳海月的忠实客户与核心合作伙伴。金蝶软件的全体 3000 多名员工，每人都配置了深圳海月的动态口令卡，用于登录金蝶的内部 OA 系统。金蝶的 ESA、K3、OA 等系列产品，内置集成了深圳海月的动态口令产品，并捆绑软件推荐给最终用户。目前，已有数万金蝶软件用户在使用深圳海月的动态口令产品。

3.5. 其他成功案例介绍

- ✓ 格力集团
- ✓ 蒙牛集团

- ✓ 伊川电力总公司
- ✓ 江苏银茂控股（集团）有限公司
- ✓ 先声药业集团
- ✓ 郴州汽车运输集团有限公司
- ✓ 新疆屯河集团
- ✓ 大连软件园股份有限公司
- ✓ 大连中床国际物流集团
- ✓ 上海宝隆(集团)股份有限公司
- ✓ 重庆渝江压铸有限公司
- ✓ 重庆工程局
- ✓ 爱施德实业股份有限公司
- ✓ 广州白云出租汽车集团
- ✓ 奥园集团

4. 售后服务

深圳海月通信向客户提供如下的服务：

1. 提供现场产品使用方面的培训服务；
2. 提供现场产品安装、调试、实施技术支持；
3. 应客户要求提供二次开发的服务；
4. 非人为损坏，一年内免费更换；
5. 一年内如果软件产品有升级，免费提供升级服务；
6. 通过电话为用户提供不限次数的系统安装、移植、测试和故障排除等问题的解答；
7. 通过邮件为用户提供不限次数的系统安装、移植、测试和故障排除等问题的解答；
8. 通过网站论坛为用户提供不限次数的系统安装、移植、测试和故障排除等问题的解答；
9. 通过网络即时通信工具为用户提供不限次数的系统安装、移植、测试和故障排除等问题的解答；
10. 为用户提供 7×24 小时的服务；
11. 支持客户将动态密码扩大应用范围。

5. 深圳海月通信公司介绍

深圳市海月通信技术有限公司是一家集信息安全领域产品研发、生产和销售于一体的创新型高科技企业。公司在国内率先推出 具有自主知识产权的“易安全”系列动态密码产品，填补了国内这一领域的空白，由此打破了该领域一直处于国外产品垄断的局面。海月通信公司推出的“数字证书＋动态密码”解决方案、“VPN＋动态密码”解决方案是业界首创和领先的解决方案。 海月通信先后与领导着中国管理软件行业的金蝶国际软件集团公司、用友软件股份有限公司总部签订了战略合作协议，与金蝶软件公司联合推出了“金蝶 EAS＋海月动态密码”解决方案、“金蝶 K3＋海月动态密码”解决方案、“金蝶 OA＋海月动态密码”解决方案等一系列解决方案；与用友软件公司联合推出了“用友 NC＋海月动态密码”解决方案、“用友 U8＋海月动态密码”解决方案、“用友 OA＋海月动态密码”解决方案等一系列解决方案。这些集“企业信息化管理”与“企业信息安全”于一体的企业整体信息系统解决方案，深受客户的好评！

海月通信拥有专业的测试队伍和完善的测试设备，“易安全”系列动态密码产品通过了中华人民共和国公安部的计算机安全产品测试，并取得了计算机信息系统安全专用产品销售许可证。

海月通信坚持“客户第一，以人为本，勇于创新，团结务实”十六字方针，每年以不低于销售收入的 15%投入产品研发，保持中国动态密码领域第一品牌的领导地位。

联系方式

深圳市海月通信技术有限公司

电话：0755-26052705

传真：0755-83661990

网址：www.seamoon.com.cn