iKEY™ 双因素动态密码身份认证系统

企业安全解决方案

上海众人网络安全技术有限公司

2009 年 5 月

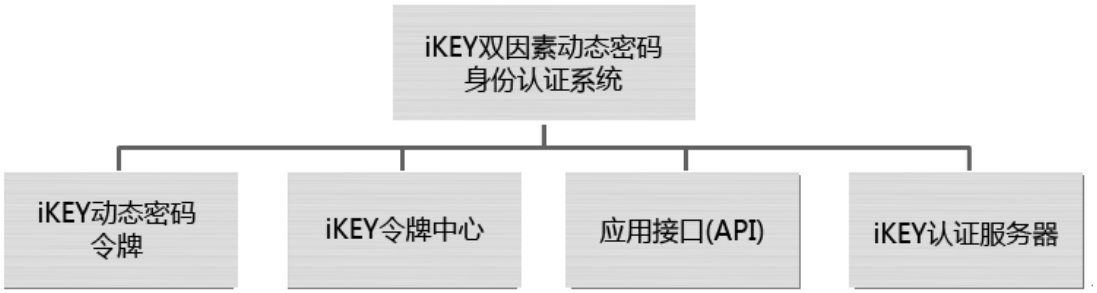
目录

一、 产品概述

“iKEY 双因素动态密码身份认证系统”是一种采用时间同步技术的双因素认证系统。“iKEY 双因素动态密码身份认证系统”采用动态的用户认证系统替代基本的口令安全机制，帮助消除因口令欺诈而导致的损失，防止恶意入侵者或人为破坏，解决由口令泄密导致的入侵问题。

“iKEY 双因素动态密码身份认证系统”采用国家商用密码管理局授权的国密算法，也可采用 ECC 国际通用标准算法。

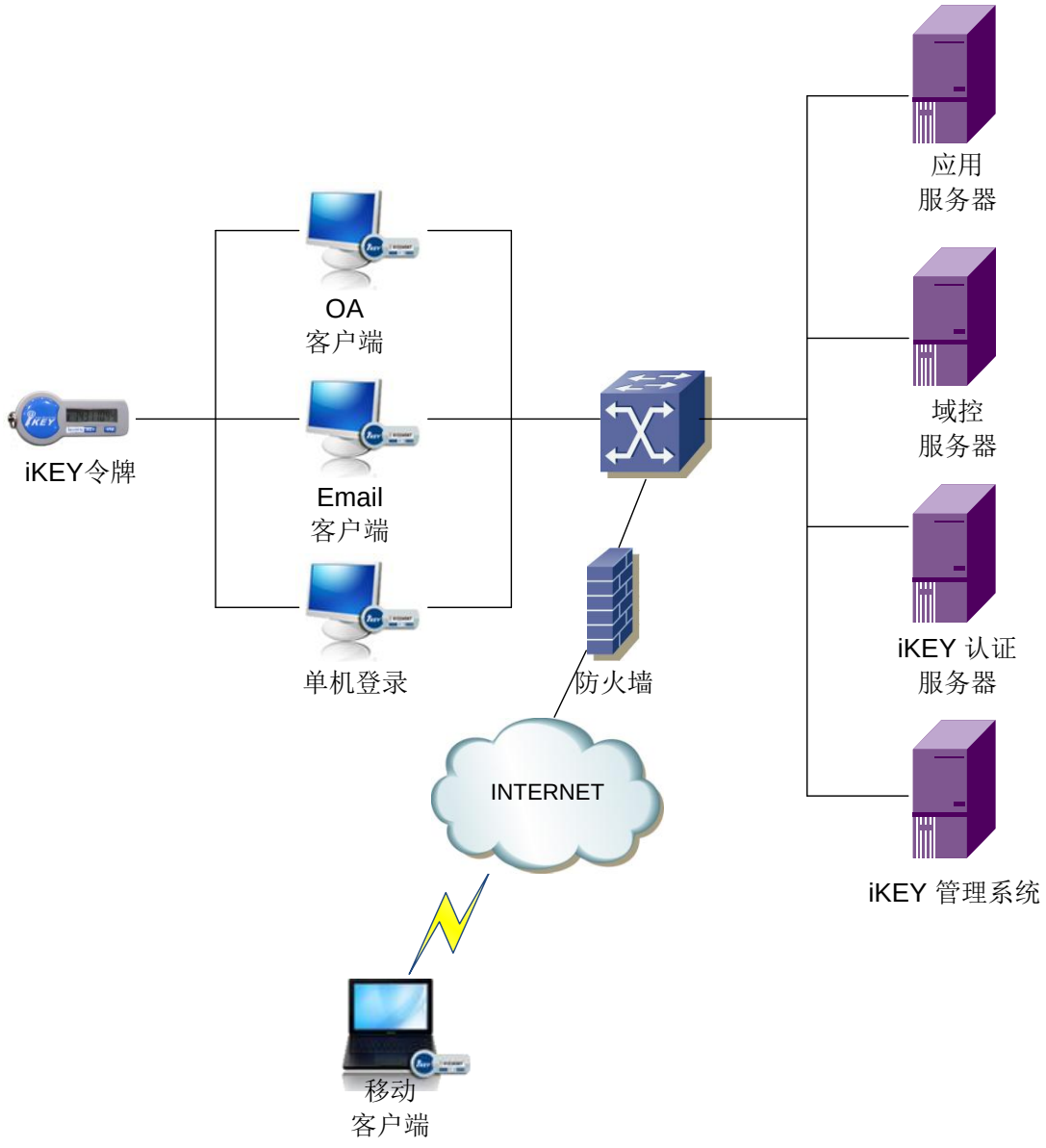
产品构成



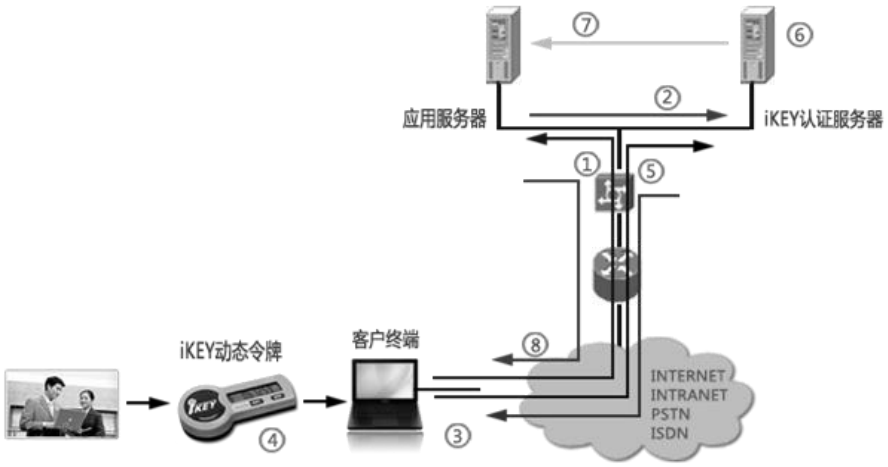
“iKEY 双因素动态密码身份认证系统”主要由 iKEY 认证服务器、iKEY 令牌中心、应用接口（API）和 iKEY 动态密码令牌四部分组成：

- **iKEY 认证服务器**：控制所有上网用户对网络的访问，提供严格的身份认证，保证上网用户根据业务系统的授权来访问系统资源。
- **应用接口 API**：应用编程接口。
- **iKEY 令牌中心**：认证服务器授权以及令牌信息导出。
- **iKEY 动态密码令牌**:以硬件形式向用户提供,可确认用户的合法身份。

二、 企业应用网络拓扑图


应用
服务器
OA
客户端
域控
服务器
iKEY令牌
Email
客户端
iKEY 认证
服务器
单机登录
防火墙
INTERNET
iKEY 管理系统
移动
客户端

三、 认证原理



步骤 1：客户请求接入应用服务器;

步骤 2：应用服务器请求认证服务器对客户的身份的合法性和真实性进行认证;

步骤 3：客户终端弹出身份认证对话框;

步骤 4：客户将账号和 iKEY 动态令牌显示的动态口令键入终端的身份认证对话框;

步骤 5：客户终端将账号和口令通过网络传输给 iKEY 认证服务器;

步骤 6：iKEY 认证服务器调用客户信息，产生与客户信息和时间相关的随机序列，并与客户输入的口令进行比对，判别客户身份的合法性和真实性;

步骤 7：iKEY 认证服务器将认证结果报告给应用服务器;

步骤 8：应用服务器根据客户身份的合法性和真实性反馈给客户终端，并决定可以提供服务或拒绝服务。

四、 产品优势

无接触：密码的产生过程完全与网络隔绝，有效杜绝了令牌密码算法、算法因子被复制、破解，从根本上保障了身份认证密码的安全性。

保密性：用户的密钥安全存储，不需在信道上传送，最大限度地防止用户身份的泄露。

抗抵赖性：只有持有动态密码产生设备的使用者能生成包含抗抵赖信息的动态密码，认证方和任何第第三方不能生成该用户的动态密码。

抗重放性：一个动态密码只能使用一次，一旦使用就立即作废。

抗暴露性：由于动态密码有使用作废和超时作废的功能，即使密码泄露，也不会出现安全隐患。

方便性：密码不需要记忆。

五、 产品技术参数

■ iKEY 认证系统部署环境

部署环境	描述
硬件平台	x86 体系服务器、小型机； 建议采用 x86 体系服务器
操作系统	操作系统 备注 Windows Windows 2000/xp/2003 Linux linux 2.4 内核以上 UNIX HP-UX 11iv2 AIX 5L 5.3 SOLARIS 10
数据库	支持符合 SQL92 标准的数据库系统；

■ iKEY 认证系统技术参数

参数项目	指标描述
可容纳用户数	1 千万~1 亿
单认证服务器处理能力	10000 次/秒
认证响应时间	<6ms/秒
认证带宽占用	<1M
认证数据冗灾	集群式备份
带外认证	支持带外认证
支持协议	对外接口协议 支持标志 TCP/SSL 认证接口协议 ☑ SOAP/HTTPS 认证接口协议 ☑ RADIUS 协议 ☑ LDAP 协议 ☑ 按客户要求定制对外接口协议 ☑

认证稳定性	最高连续满功率运行认证次数 10，000，000，000 次
认证正确性	连续满功率运行时正确率大于 99.99999999%
支持动态口令长度	6-8 位
PIN 码功能	支持
密钥自助写入	支持

■ 动态令牌硬件技术参数

参数项目	指标描述
尺寸（长×宽×高）	57.5*27*8.7MM （外形客户可定制）
重量	约 20 克
电池条件	220MAH 纽扣电池
电池寿命	3 年
工作环境温度	-10℃~+50℃
存储环境温度	-25℃~+70℃
工作环境相对温度	10%-90%，非凝结
防震	符合 GB/T 2423.10，GB/T 2423.11，GB/T 2423.12，GB/T 2423.13，GB/T 2423.14，GB/T 2423.15
防干扰	符合 GB 4343.1-2003
防水	达 IP68 等级
防拆	采用国家商用密码管理局指定安全算法芯片，具备防非法读写的功能
注胶	低压注塑

六、 关于众人

1. 公司简介

- 上海众人网络安全技术有限公司（以下简称“众人网络”）于 2007 年 9 月在张江高科技园区国家信息安全基地成立，注册资金 3000 万元人民币。
- “众人网络”研发团队成员 70%以上具有研究生以上学历，且拥有从事国内外知名 IT 企业和研发机构关键性技术职务的经历。“众人网络”已与交通大学、武汉大学等国内著名高校建立的稳定的战略合作关系，以强大的产学研一体化基地三大优势为后盾，不断汇聚国内顶尖网络安全技术领域的菁英，为推动中国网络安全事业发展做出贡献。
- 2008 年 5 月，“众人网络”成为国家密码管理局指定的商用密码产品生产及销售定点单位，是国内首家（目前唯一）获得国家密码管理局批准生产和销售列入《商用密码通用产品名单》的动态密码产品的合法企业。
- 2008 年 12 月“众人网络”的身份认证产品“iKEY 双因素动态密码身份认证系统”被中国企业创新成果案例审定委员会评为“最具自主创新能力企业成果(案例)”，并通过了上海市高新技术成果转化项目 A 级认定。
- “众人网络”致力于帮助广大计算机个人用户、企业和政府机构保护信息安全；并提供身份认证、信息访问控制、交互管理等企业级、银行级专业安全解决方案。

2. 专家顾问

- 王椿芳（将军/研究员）：中国人民解放军国家有突出贡献的密码专家，曾担任国家级安全部门顾问，荣获国家科技进步一等奖、二等奖。现任“众人网络”专家顾问团总顾问。
- 李建华（教授）：上海交通大学信息安全工程学院常务副院长、教授、博士生导师，上海市信息安全综合管理技术研究重点实验室主任，哈尔滨工程大学信息安全研究中心主任、兼职教授、博士生导师。曾任国家电子政务试点示范工程总体专家组专家、国家十五重大科技攻关计划任务国家信息安全应用示范工程—‘S219 二期工程’” 总体组组长、“国家十五 863 计划信息安全技术发展战略”专家组核心科学家。现任“众人网络”专家顾问团高级顾问。

3. 资质与荣誉

- **企业资质**
  - 08 年 5 月，获得了由国家密码管理局颁发的《商用密码产品生产定点单位证书》；
  - 08 年 9 月，获得了由公安部公共信息网络安全监察局颁发的《计算机信息系统安全专用产品销售许可证》；
  - 09 年 1 月，获得 ISO9001：2000 质量管理体系认证和 ISO27001 信息安全管理体系认证，是中国大陆地区信息安全企业中首家通过权威机构 SGS ISO27001 认证的企业。

- 09 年 2 月，“iKEY 双因素动态密码身份认证系统”通过国家密码管理局安审，获得《商用密码产品型号证书》；
- 09 年 2 月，获得了由国家密码管理局颁发的《商用密码产品销售许可证》。

■ **产品通过的权威检测**

- “iKEY 双因素动态密码身份认证系统”通过国家商用密码管理局安审产品检测；
- “iKEY 双因素动态密码身份认证系统”通过公安部计算机信息系统安全产品检测中心检测；
- “iKEY 双因素动态密码身份认证系统”通过上海市计量测试技术研究院、华东国家计量测试中心、中国上海测试中心产品检测；
- iKEY 双因素动态密码令牌通过美国摩尔实验室 FCC、CE 和产品整体性能检测；
- “iKEY 双因素动态密码身份认证系统”通过上海市软件评测中心 5000 万用户、单台服务器认证并发万次每秒性能测试。

■ **企业荣誉**

- 08 年 12 月，“iKEY 双因素动态密码身份认证系统”通过上海市高新技术成果转化项目 A 级认定；
- 08 年 12 月，在天津举办了中国中小企业协会“2008 中国企业创新成果（案例）”评选活动暨第二届中国中小企业节。经中国企业创新成果案例审定委员会审定，“众人网络”的“iKEY 双因素动态密码身份认证系统”在此次评选活动中荣获“最具自主创新能力企业成果(案

例)”。

- “众人网络”成为“中国中小企业协会”副会长单位。中国中小企业协会是全国中小企业、企业经营者自愿组成的全国性、综合性、非营利性的社会团体。中国中小企业协会接受国家发展和改革委员会业务指导和民政部的监督管理。
- “众人网络”成为“上海市信息安全行业协会”理事单位。协会的业务主管单位是上海市信息化委员会和上海市行业协会发展署。我公司负责协会的信息安全产品测试平台的身份认证环境搭建并提供相关技术支持，以及编写培训教材《商用密码应用技术基础》的身份认证技术章节。
- “众人网络”成为《上海信息化》杂志协会理事单位。