# 深圳竹云科技有限公司

# 竹云 e 登录白皮书

Bamboocloud elogon Product White Paper

编号：BBC-WP-ELogon-2018001

版本：1.0

深圳竹云科技有限公司

2018 年 4 月

# 目录

# 1 背景

随着企业信息化水平的提高与电脑的普及，目前大多数企业采用 Windows 操作系统作为电脑桌面进行信息化办公。企业中的每台电脑或多或少均存有与企业相关的资料、数据，这些信息通常是敏感的、关系到企业发展与利益的、不希望能被非法访问的。企业除了设置物理安全（门禁）以外，访问这些敏感信息的最后一道屏障就是 Windows 系统的用户名与密码组合。一旦有不法人员获取了用户名与密码，并突破了物理限制，就能轻松的访问电脑中的敏感数据，对企业造成无法估量的损失。随着企业对信息化安全程度的要求越来越高，传统的、基于用户名与密码组合的登录方式无法再满足企业对敏感数据的安全性要求。

Windows 操作系统在登录时主要面临的威胁：

- 仅使用单一密码验证身份，安全性差
- 如果密码设置的较为简单，则容易被猜到
- 为了提高安全性，可能设置了复杂的密码，不仅不便于记忆，且登录过程繁琐
- 密码存在被黑客工具暴力破解的概率
- 任何人只要知道了某台电脑的密码，即可登录他人系统
- 缺乏安全的多因素身份认证机制
- 无法将人员与密码精确匹配，存在密码被共用的风险
- 缺乏统一的安全审计、考勤、行为分析等过程
- 虽然 GPO 可以限制登录时间，但无法实现较复杂的登录策略

# 2 产品介绍

## 2.1 概念和术语

Windows: 微软视窗操作系统

Active Directory：微软活动目录产品产品，实现了基于网络的计算机目录服务

Kerberos：一种目录服务安全身份验证协议

COM：操作系统底层通讯接口

UI：用户界面

OTP: One-time Password，也称动态口令，是根据专门的算法每隔 N 秒生成一个与时

间相关的、不可预测的随机数字组合

## 2.2 产品描述

安全 e 登录系统（以下简称 e 登录），是一套专门用于增强 Windows 身份认证安全性的整体解决方案。

e 登录可以在原有 Windows 身份认证的基础上，实现手机令牌身份认证、手机短信身份认证、U 盘身份认证、数字证书 U 盾身份认证，以及扩展其他生物认证方式等，极大增强了 Windows 身份认证过程的安全性，从而提高企业整体信息化的安全等级。

e 登录不仅可以作为单机产品独立运行，也可以与局域网、Active Directory 紧密集成，扩展实现定制的安全认证方式；还可以与企业现有系统（如防火墙、HR 系统）扩展集成，实现复杂的安全认证策略与行为审计。

## 2.3 特点和优势

- 支持多因素身份认证机制、超强安全性
- 支持用高级的身份认证方式（令牌、短信、U 盾等）取代传统的密码认证方式
- 杜绝密码被破解、猜测、共用的风险
- 即使密码遭遇泄露，也不影响系统安全
- 登录人员与登录系统的精确匹配
- 用户无需记忆复杂的密码且进行繁琐的输入
- 配置、部署简单灵活，有单机版与网络版可供选择
- 实现统一安全策略、统一安全审计、用户行为分析等
- 支持进行扩展定制，实现企业特殊信息安全要求

# 2.4 系统架构

## 2.4.1 整体架构

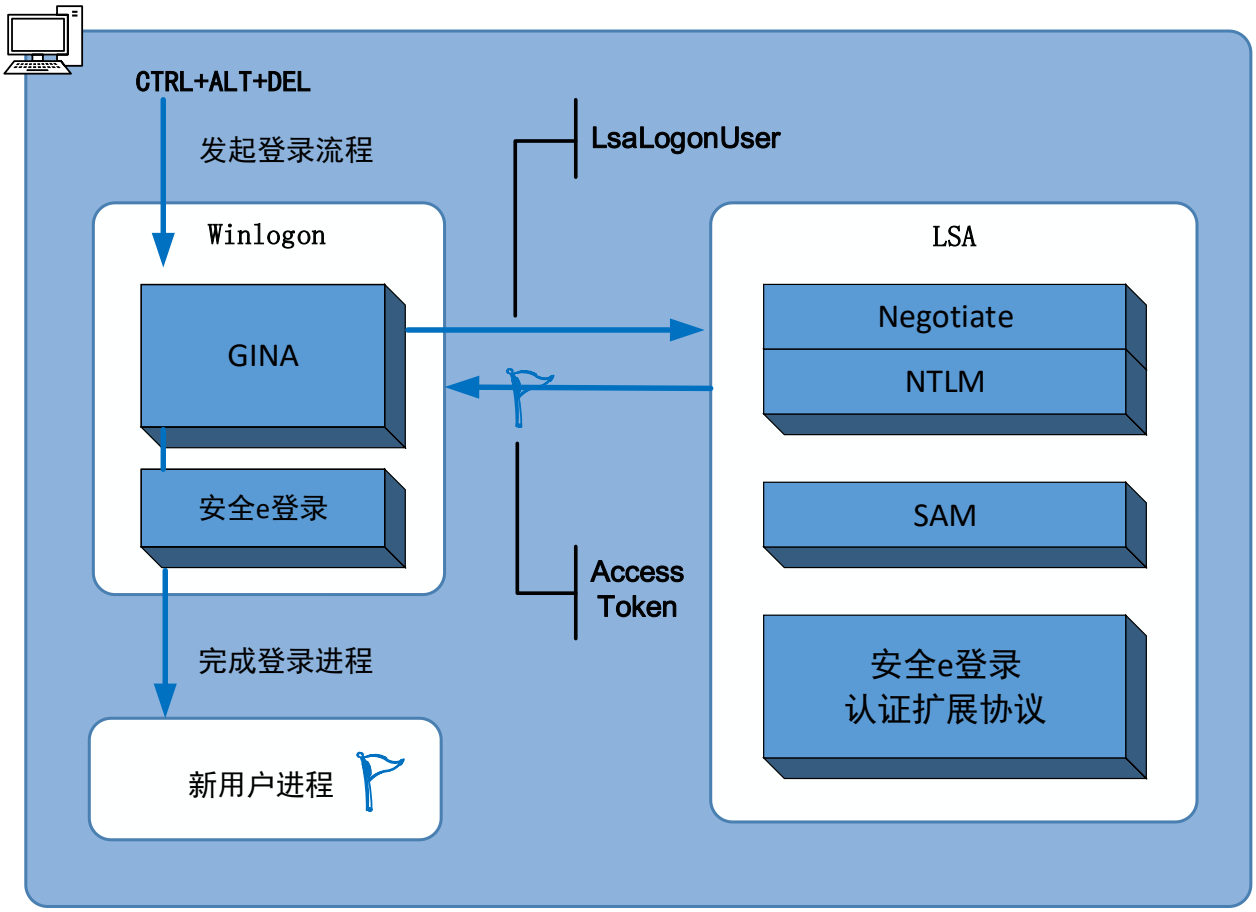


图 1 整体架构

安全 e 登录系统在现有 Windows 认证架构的基础上，增加了凭据提供者、扩展协议栈，以及相关附加组件。

- **凭据提供者**

凭据提供者是一组 COM 接口，是用户进行身份认证的主要机制，是用户在登录时证明身份的唯一方式。

Windows 凭据提供者框架允许扩展第三方凭据提供者。当 Winlogon 进程想要收集用户凭据时，Logon UI 首先查询凭据提供者，并获取相关信息，然后 Logon UI 根据凭据提供者返回的信息渲染 Logon UI，并最终呈现给终端用户。凭据提供者允许用户输入相关凭据信息，Logon UI 会提交这些信息进行后续身份验证。

➢ **扩展协议栈**

扩展协议栈包含了一组扩展身份认证方式，如动态口令 OTP（One-time Password）认证、手机短信 SMS 认证、USB Disk 加密认证、数字证书 U 盾认证等。

这些新增的认证方式不仅可以直接取代原有的 Windows 认证方式，也可以与原有 Windows 认证方式组合使用，形成多因素认证，进一步提高系统安全性。

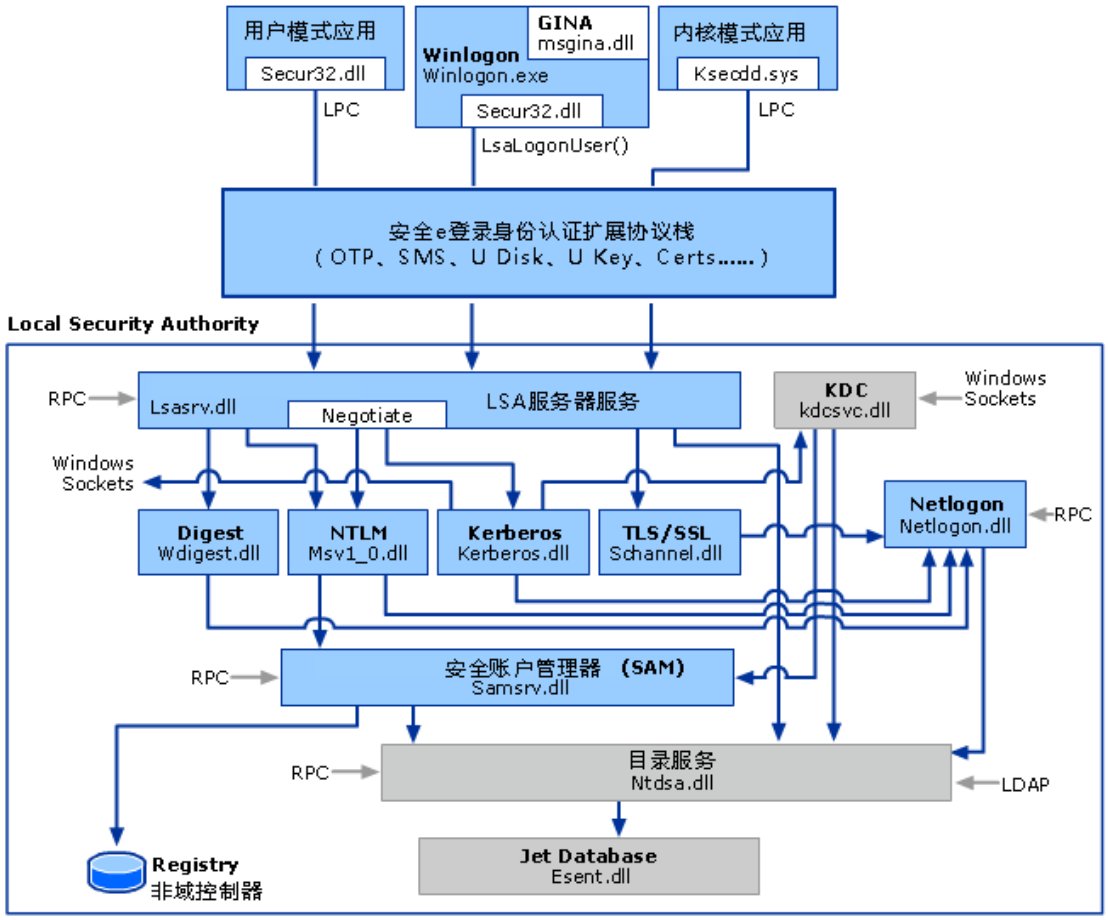


图 2 扩展协议栈

➢ **安全 e 登录认证流程**

1. 用户按下 Ctrl+Alt+Del 组合键；
2. WinLogin 进程接收 SAS 消息，并调用 GINA 进行处理；
3. GINA 调用 e 登录凭据提供者，注册相关监听事件，渲染登录界面；
4. e 登录凭据提供者收集用户凭据，发送至 e 登录扩展协议栈；
5. e 登录扩展协议栈处理凭据信息、检测用户环境、初始化外部设备、建立网络通讯；

6. e 登录扩展协议栈验证凭据是否有效，返回 success 或 failure；
7. 如果返回 success，则继续将凭据信息发送至 LSA；
8. LSA 协商路由至 Kerberos，Kerberos 无法处理本地登录，则协商路由至 NTLM；
9. 验证凭据是否有效，LsaLogonUser 调用返回 success 或 failure；
10. 如果返回 failure，则 GINA 提示用户输入有效的凭据；
11. 如果返回 success，则 GINA 激活用户会话，登录成功。

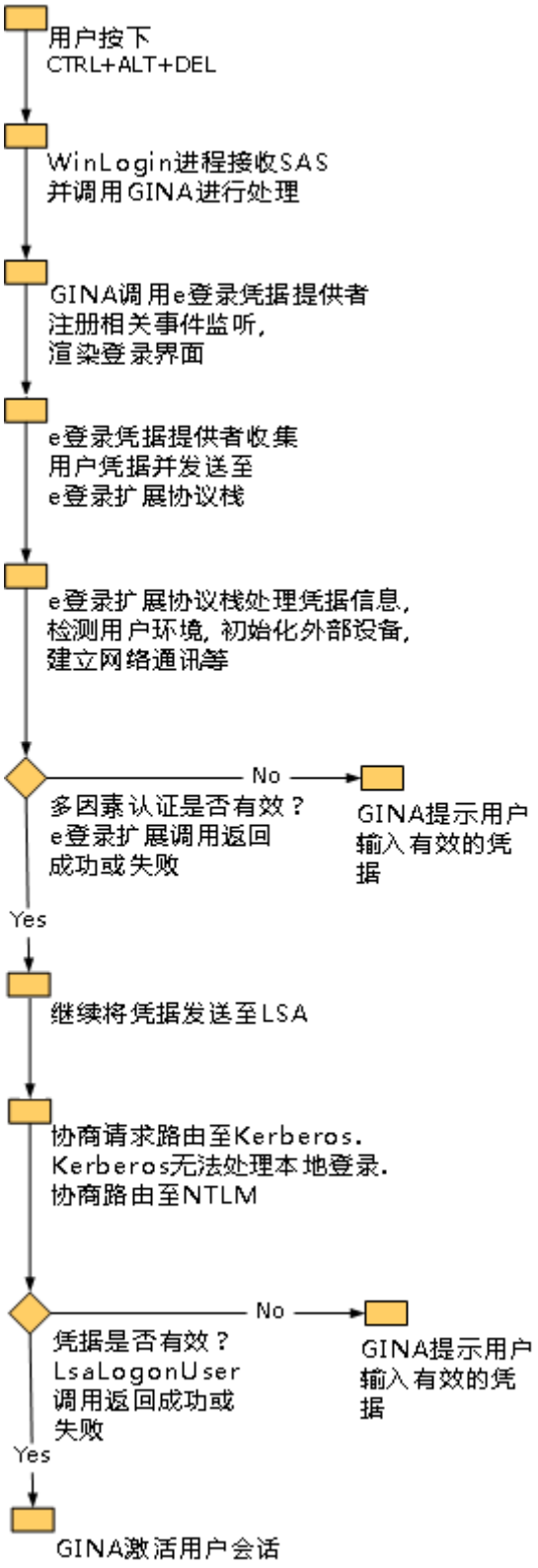


图 3 e 登录认证流程

## 2.4.2 兼容性

- **软件环境要求：**.NET 4.0、VC++ 2010 运行库
- **操作系统要求：**

·Windows 7 64 位

·Windows 7 32 位

·Windows 10 64 位

·Windows 10 32 位

·Windows XP 32 位

·Mac OS/OS X

### 2.4.3运行环境

- **最低配置要求：**

·CPU: 1GHz

·内存：512MB

·硬盘：500MB 剩余空间

- **建议配置要求：**

·CPU: 2GHz

·内存：2GB

·硬盘：1GB 剩余空间

## 2.5 主要功能介绍

### 2.5.1OTP 认证

OTP 认证使用基于时间的算法产生一组随机的动态口令，并在竹云 OTP 手机客户端展示；用户输入动态口令进行身份验证，登录 Windows 系统。

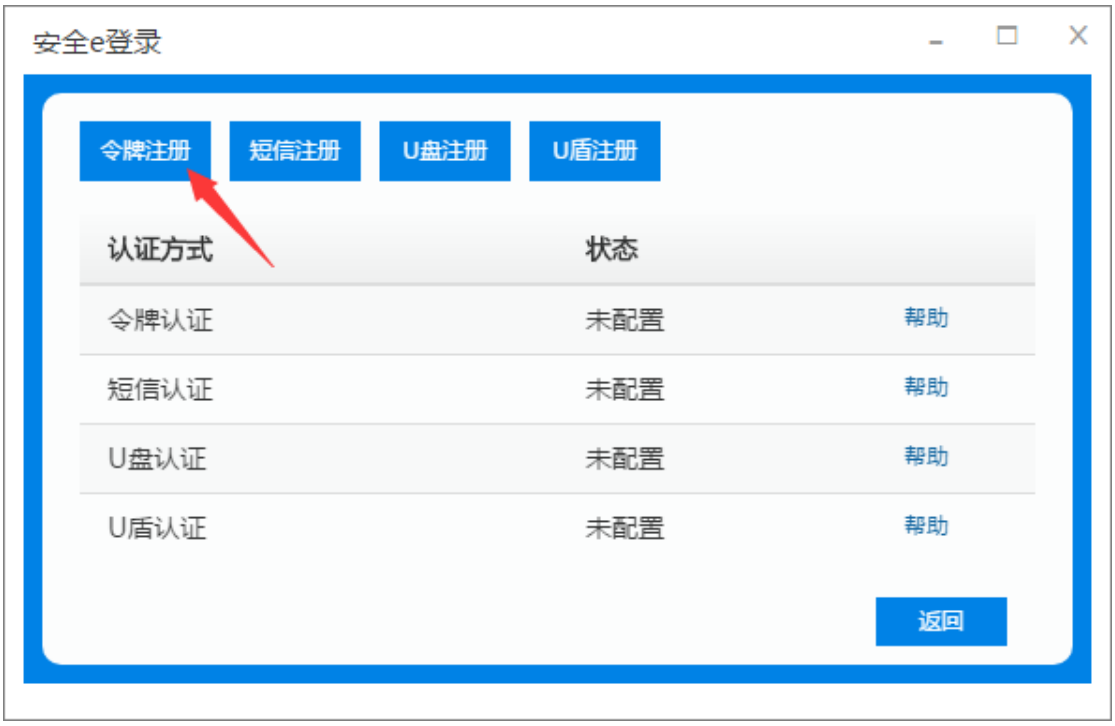


图 4 OTP 认证令牌注册示意图 1


图 5 令牌注册示意图 2


图 6 令牌注册示意图 3

### 2.5.2 短信认证

短信认证通过调用短信网关（电信、联通、移动），向用户手机发送短信验证码；用户输入收到的短信验证码进行身份验证，登录 Windows 系统。

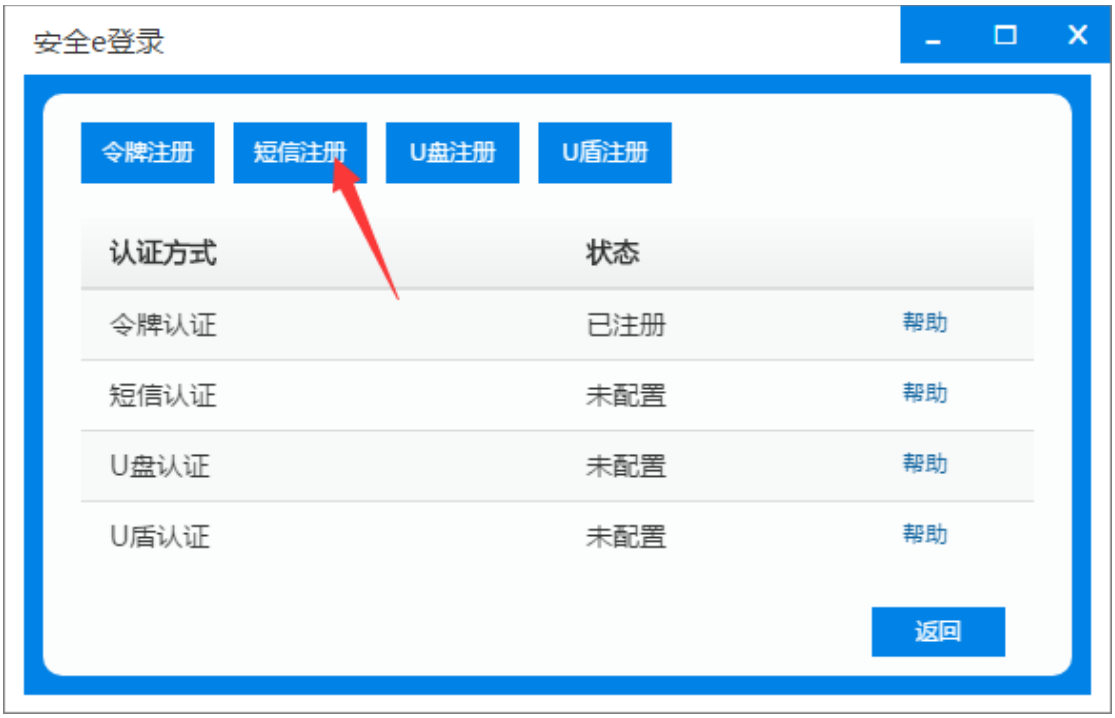


图 7 短信认证示意图 1

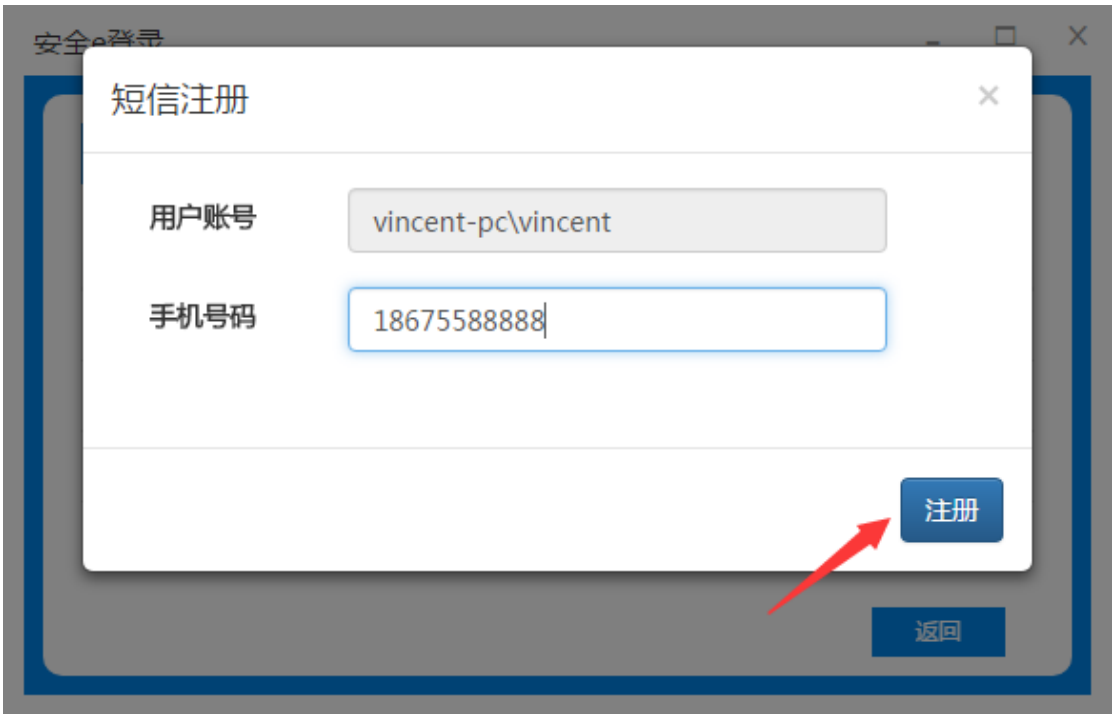


图 8 短信注册

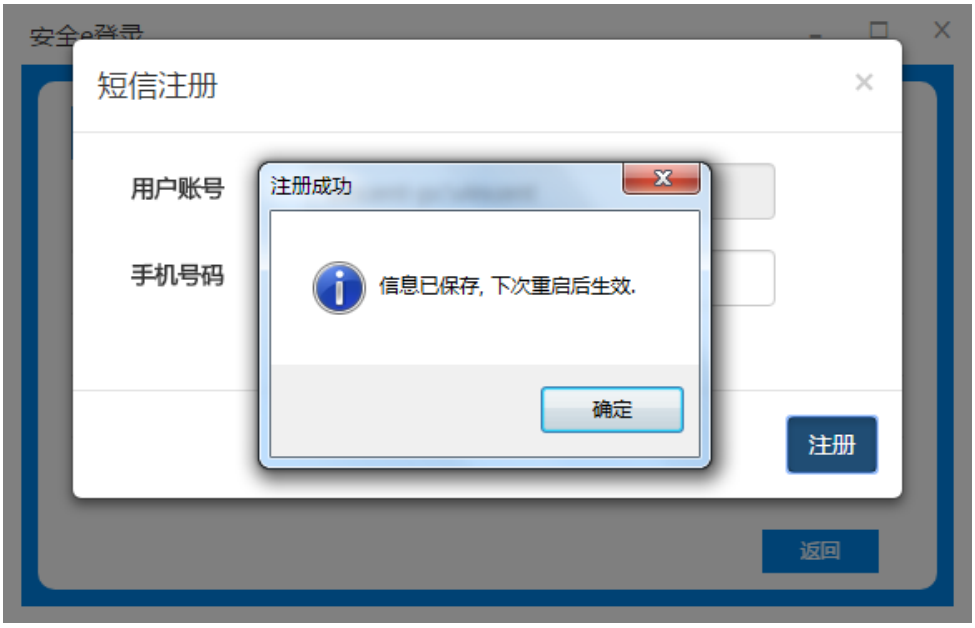


图 9 短信注册示意图 3

### 2.5.3U 盘认证

U 盘认证使用一组加密算法，并结合 U 盘的物理信息，向 U 盘写入加密数据；用户在计算机插入 U 盘进行身份验证，登录 Windows 系统。

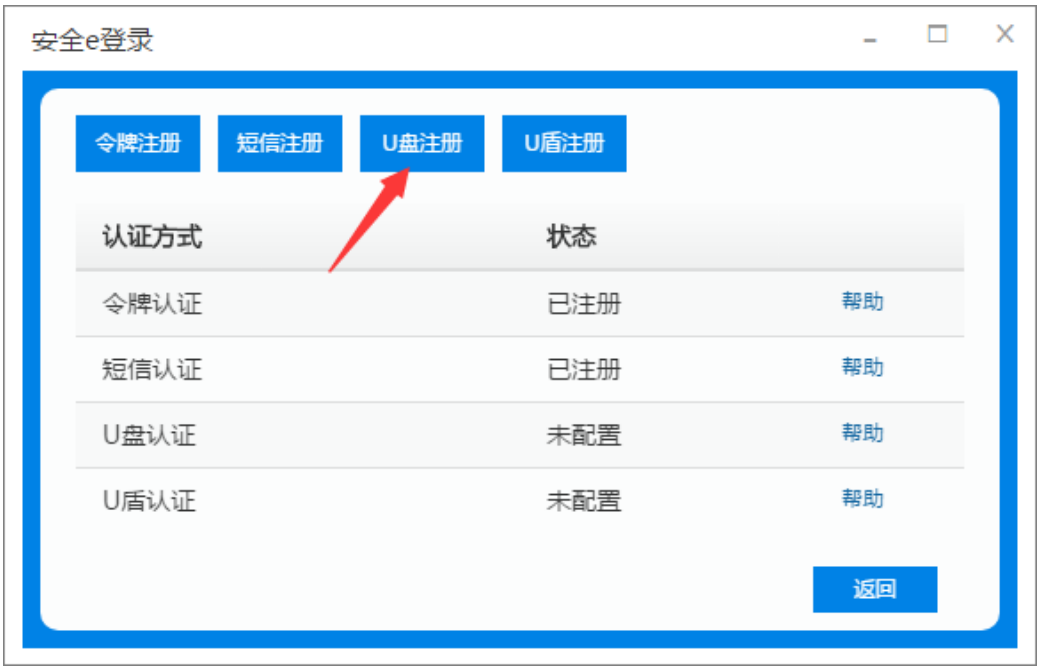


图 10U 盘认证示意图 1

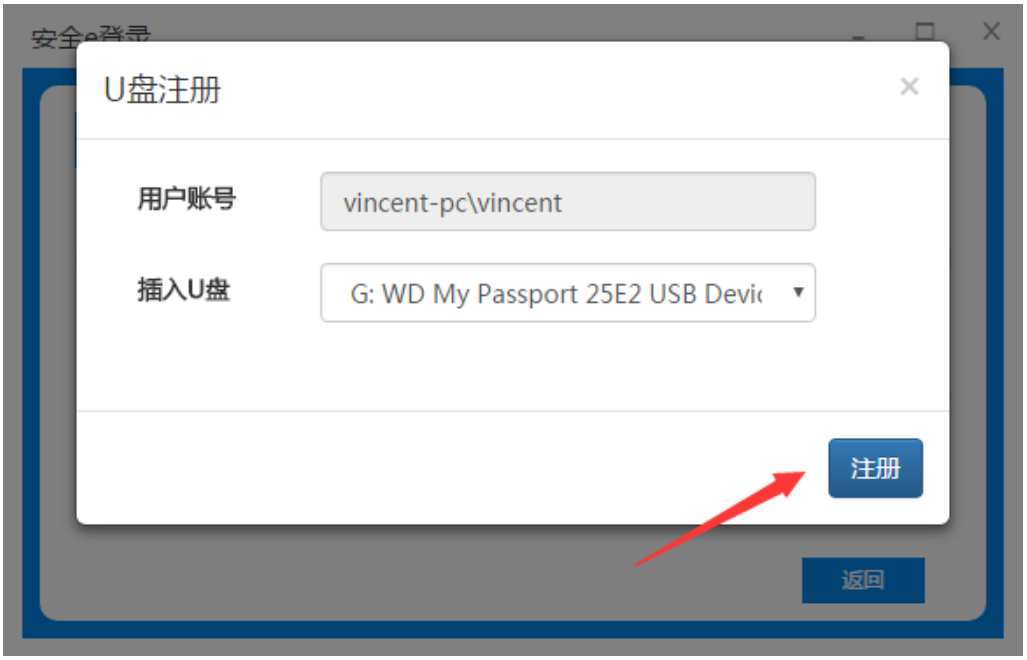


图 11 U 盘注册示意图 2

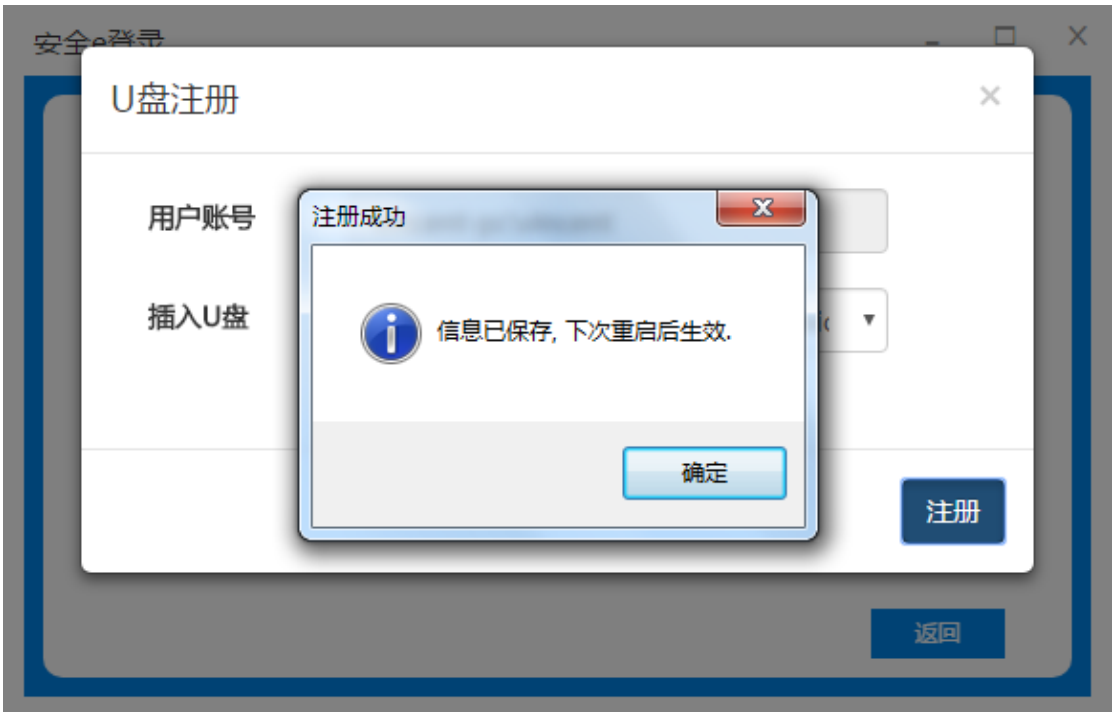


图 12 U 盘注册

## 2.5.4U 盾认证

U 盾认证使用北京数字证书认证中心的 UKey 硬件产品，并结合数字签名、数字证书、非对称密钥等技术；用户在计算机插入 U 盾进行身份验证，登录 Windows 系统。

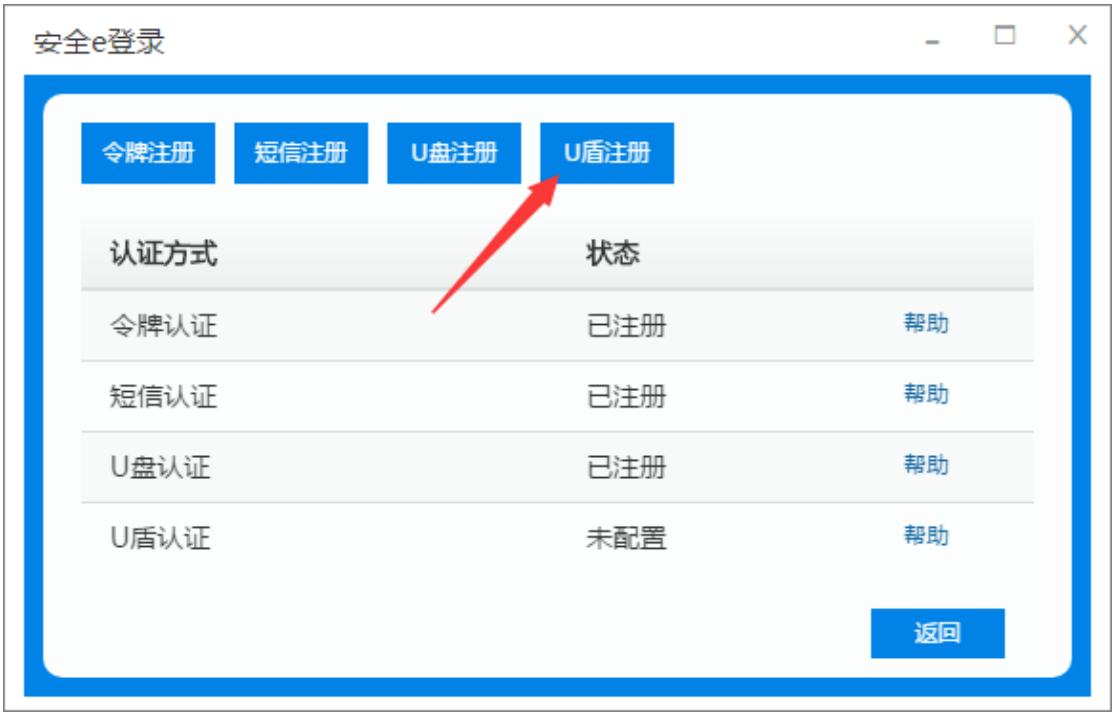


图 13 U 盾认证注册


图 14 U 盾认证账号注册

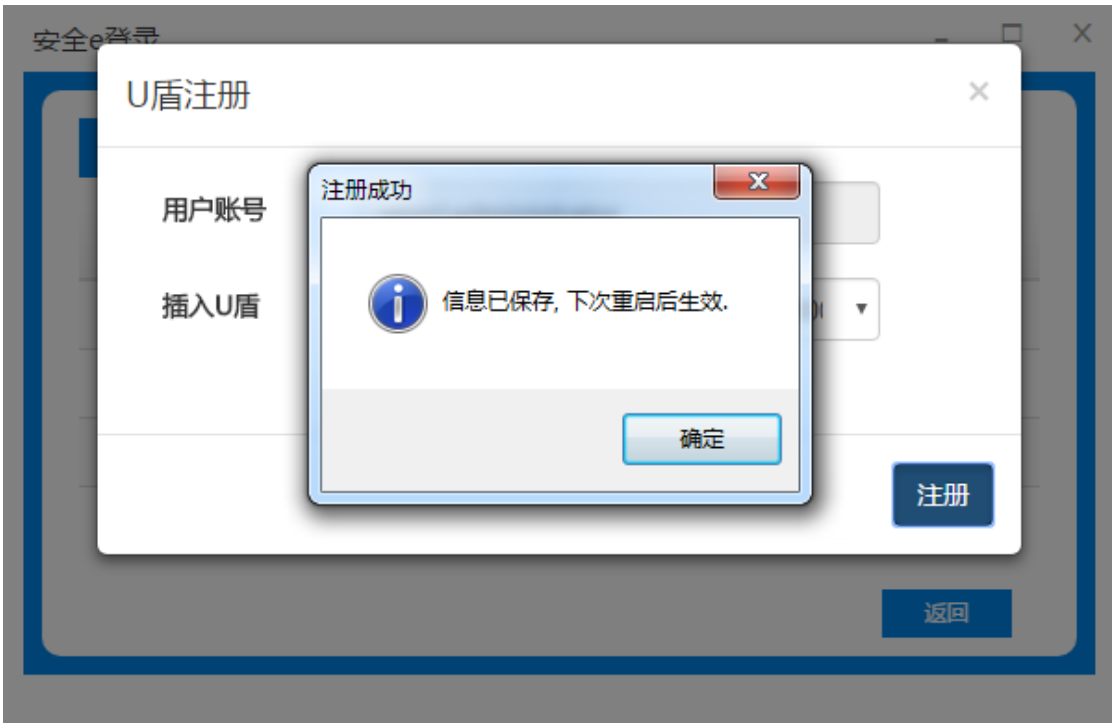


图 15 U 盾注册生效

### 2.5.5 e 账通认证

通过使用竹云 e 账通手机 APP，可以获得更多的认证方式支持：人脸、声纹、指纹等，进一步提高身份验证与访问控制的安全性等级。


图 16 竹云 e 账通注册

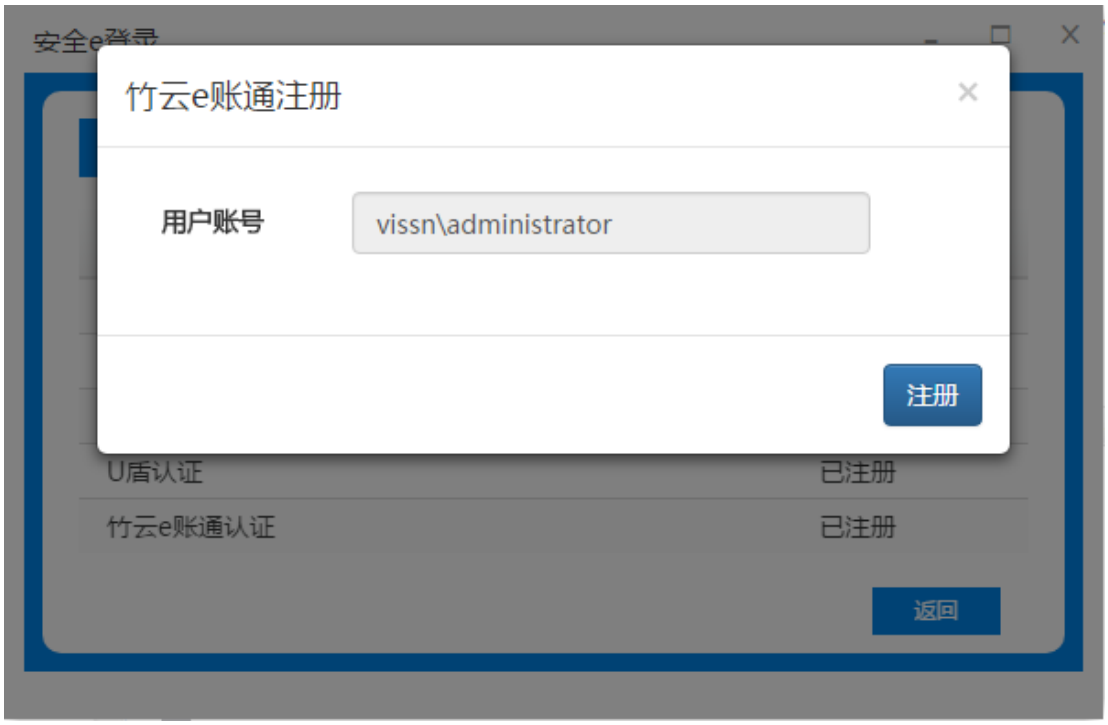


图 17 竹云 e 账通用户账号注册


图 18 竹云 e 账通二维码扫描

# 3 产品部署

e 登录支持以下安装方式：

- 直接在目标计算机上安装 e 登录客户端，无需输入服务端地址，e 登录将以单机版方式工作。

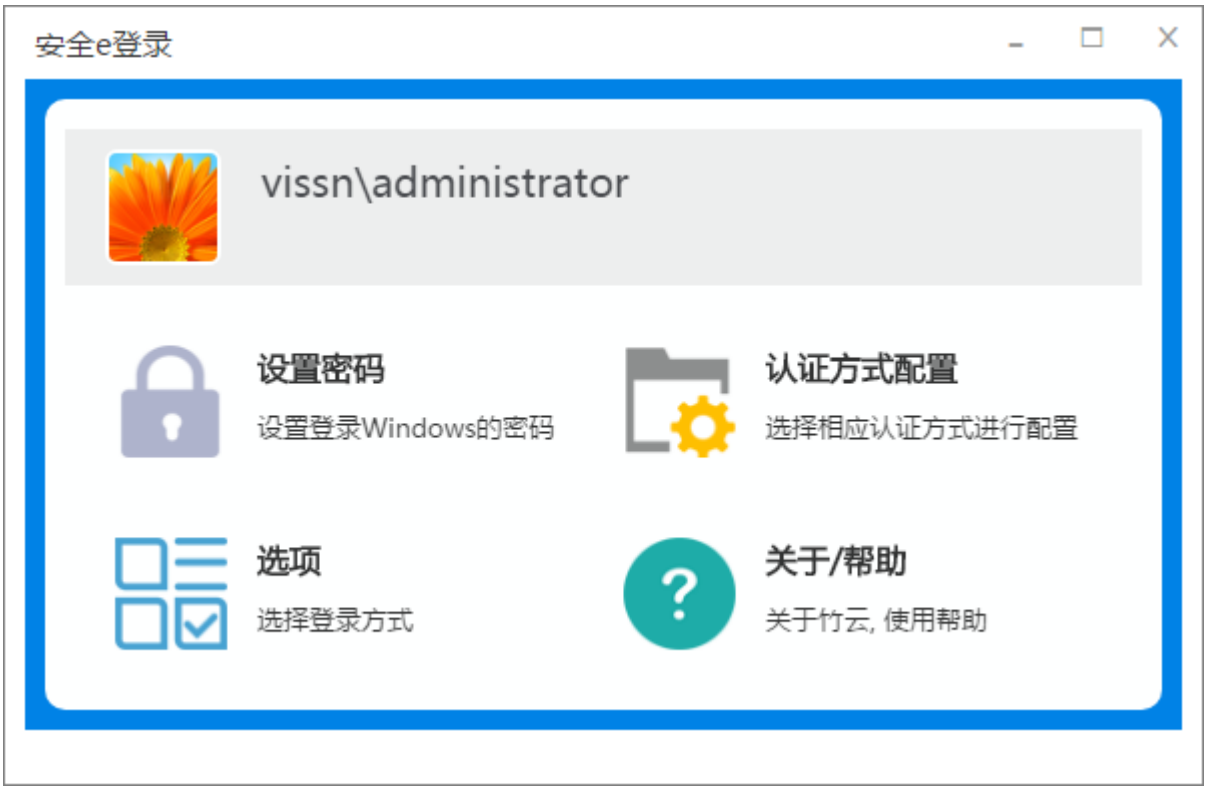


图 19 产品部署界面示意图 1

➢ 在局域网内部署 e 登录服务端并配置，同时在客户机上安装 e 登录客户端，并输入服务端地址，e 登录将以网络版版方式工作。

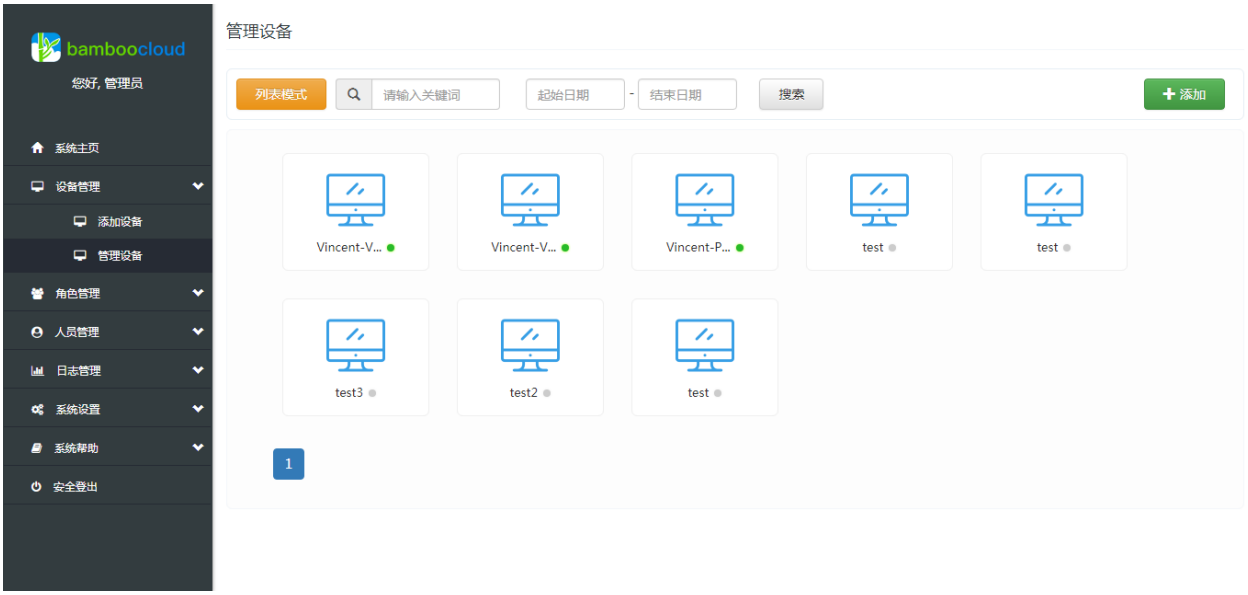


图 20 管理界面

# 4 产品集成

e 登录支持以下集成方式：

- 在用户登录 Windows 之前，由其他产品进行身份验证，并通知 e 登录自动登录 Windows 系统。
- 在用户登录 Windows 之后，可以与其他产品进行集成，授予其他应用的访问权限等；或向其他应用提交当前用户的各种信息，如行为审计等。