

金蝶企业安全认证解决方案

金蝶软件（中国）有限公司

二〇一二年八月

方案背景

- 企业需要管理不同业务系统的用户，导致了用户管理的复杂度增加和效率降低，为此企业需要付出更多的 IT 管理成本。
- 业务系统繁多，用户需要记忆多个帐户和口令，无形中引导客户使用弱密码，不同系统登陆和使用极为不便，同时由于用户口令遗忘而导致的支持费用不断上涨；
- 不同业务系统无法实现统一的安全认证和授权，同时各个系统安全策略设置级别不一致，从而无法保障各个系统的身份认证和访问安全的可靠性。

解决方案概要

方案帮助企业实现基于用户统一登陆管理、多种身份认证方式的接入，构筑企业信息安全的基础，确保业务在获取授权情况下的统一可靠的安全访问策略，可使企业获得可靠的效率和值得信赖的安全性。

■ 用户统一访问管理

在多个应用系统中，通过金蝶 SSO（单点登录），用户只需要登录一次就可以访问所有相互信任的应用系统，实现以下功能：

- 统一的用户管理
- 统一认证
- 简化用户登录流程
- 身份认证和权限认证分离

■ 身份与安全认证

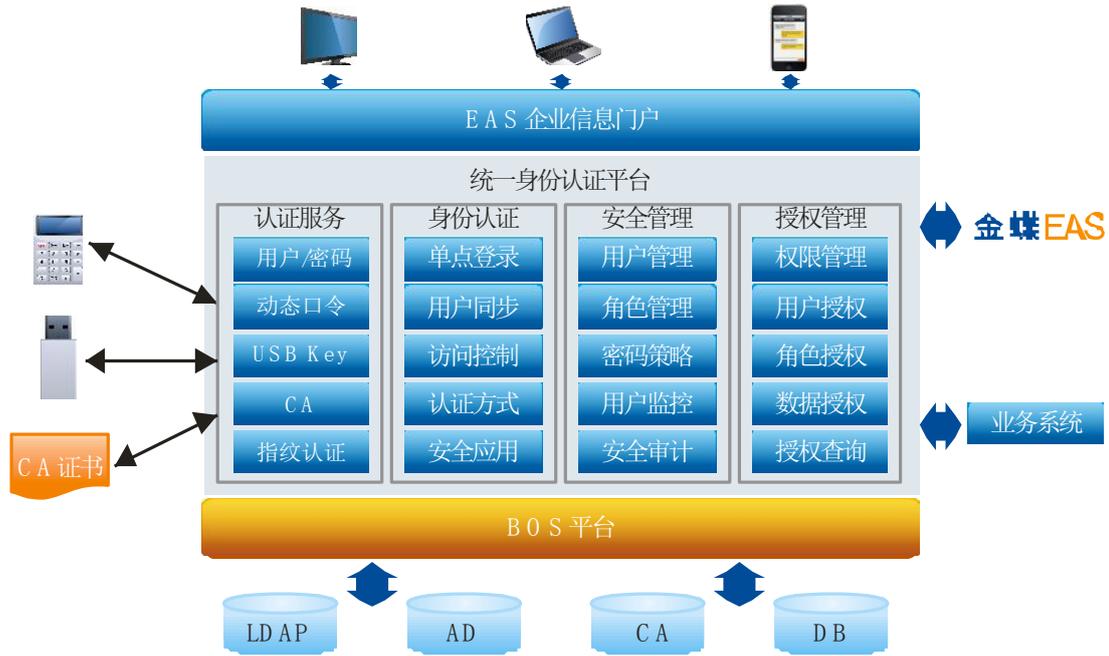
通过动态密码卡，CA 证书等实现身份与安全认证管理。

-动态密码卡：密码生成的手持终端设备，基于硬件密码种子、时间和事件，定时随机生成一个密码，具有很强的随机性、不可猜测性；

-CA 认证：CA (数字证书认证中心)是指发放、管理、废除数字证书的机构。CA 认证确保了持有证书的用户才可登陆系统。

■ 关键数据安全保障

系统通过 CA 证书可以提供数字签名服务并对数据签名结果进行真实性、有效性验证。系统可对企业财务资金以及电子商务活动中的关键敏感数据进行签名并验证，防止数据遭到非法访问和篡改，保证数据的真实性、完整性、合法性。



客户价值

金蝶企业安全认证解决方案为企业的信息安全保驾护航，提供企业稳定增长的保障：

- 建设统一的登录入口，通过动态密码和 CA 证书访问认证，大大降低用户密码泄漏风险；
- 确保访问用户身份的合法和有效性，为企业应用的访问身份安全提供了有效的保障；
- 关键敏感数据的数字签名并验证，有效保证企业对关键业务数据的全方位安全要求；

成功客户

