格尔数字证书认证系统

（SZT0901/SYT0901）

产 品 白 皮 书

上海格尔软件股份有限公司

上海格尔安全科技有限公司

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

版权声明：

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

目 录

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

1 概述

1.1 背景

随着我国电子商务、电子政务等网络应用的快速发展，越来越多的机构和企业正在构建以 PKI（Public Key Infrastructure,公钥基础设施）为基础的网络安全信任体系。PKI 体系的核心是数字证书认证中心 CA（Certificate Authority）及由 CA 颁发的数字证书。和现实社会的身份证一样，数字证书是网络世界的身份证，并进一步实现敏感信息的机密性、完整性及不可抵赖性。因此，数字证书认证机构是网络安全信任体系的基石。

目前，我国数字证书认证机构按照应用环境/范围大体可分为以下四类：区域类、行业类、商业类和内部自用（企业）类。区域类数字证书认证机构大多以地方政府为背景、以公司机制来运作，主要为本地行政区域内电子政务业务与电子商务业务发放证书；行业类数字证书认证以部委或行业主管部门为背景，以非公司机制或公司机制运作，在本部委系统或行业内为电子政务业务和电子商务业务发放证书；商业类数字证书认证以公司机制运作，面向全国范围为电子商务业务发放证书；内部自用类数字证书认证，主要是企业事业单位自建的证书机构，为自身内部业务发放证书，不向公众提供证书服务。

PKI 体系概念在安全领域得到的广泛认同，使国内越来越多机构、企业在进行网络安全建设时将 PKI 基础设施和 PKI 应用列为重要的基本组成部分，针对这样的情况国密办也适时推出了国内大型数字证书认证机构建设的标准。格尔软件在 PKI 体系建设方面积累了丰富的经验，格尔数字证书系统结构严密、功能强大、稳定可靠，系统由密钥管理系统(KM)、证书认证系统（CA）、证书注册系统（RA）、证书状态在线查询系统（OCSP）、时间戳系统(TSA)、证书综合服务系统（CDS）、证书助手（PC 端和移动端）等子系统组成完整的 PKI 公钥基础设施，该系统同时支持 SM2 和 RSA 算法，提供完备的数字证书全生命周期的管理。该系统在我国得到广泛应用，为国家网络信任体系建设、为电子商务和电子政务的信息安全体系建设发挥了重要作用。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

随着国家标准密码算法(SM1、SM2、SM3、SM4)的发布，格尔软件第一时间发布了适用于国家标准密码算法的格尔数字证书认证系统产品，并在 2009 年参加了产品的安审和鉴定，获得相关的资质和证书(SZT0901、SYT0901、SRT0903)，成为获得国家标准密码算法支持的公钥基础设施产品提供商。

SM2 算法作为一种高安全性、高效率的公钥密码算法，具备和 RSA 算法同样的加/解密、电子签名和密钥协商等重要的密码功能。与 RSA 相比，其拥有更强的安全性、更高的实现效率、更优实现代价的优点，被公认为下一代的公钥密码。

椭圆曲线公钥密码体制具有最高的位安全强度，进一步加快了运算速度，缩短了数据传输的时间。考察我国目前信息产业发展情况，SM2 算法技术和产品在电信、网络、金融、证券、军事、公安、税务等行业和政府部门有广泛的应用前景，在电子政务、电子商务、第二代居民身份证、银行 EMV2000 迁移和公安部金盾工程等重大信息化工程项目中有实际的应用需求。在介质存储空间及运算能力受限的应用场合，通过格尔数字证书认证系统(SZT0901)产品生成的 SM2 密钥证书具有明显优势。

1.2 名词解释

- CA（Certificate Authority）：证书授权机构，负责颁发、公布和废除证书，并提供诸如证书暂停服务的可以信赖人员（自然人或组织）；
- RA（Registered Authority）： 注册授权机构，负责向申请证书的人员或组织提供身份注册，审核的机构；
- KM：密钥管理中心，提供对生存周期内的加密证书密钥对进行全过程管理的功能。
- CDS：数字证书综合管理系统，提供对终端（PC 端和移动端）的证书管理。
- TSP（Time Stamp Protocol）：时间戳协议。
- OCSP（Online Certificate Status Protocol）：在线证书状态协议。
- KCM：证书助手，终端个人证书发放和使用，支持运行在 PC 端和移动

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

端，替代传统 online 的模式，使用证书助手可支持 SM2 证书的应用。

- X.509v3：是由 IETF 提出的公开密钥基础架构规范的第三版；
- PKI（Public Key Infrastructure）：公开密钥基础架构；
- 明文（plaintext 或 message）：未经加密的原始数据；
- 加密（encryption）：用某种方法伪装数据的过程；
- 密文（ciphertext）：加密后的数据；
- 解密（decryption）：将密文还原为明文的过程；
- 密码算法（algorithm）：用于加密或解密的数学函数，简称算法。通常包括两个函数，一个用于加密，一个用于解密。如果密文的安全依赖于算法的保密，这种算法称为受限制的（restricted）算法；如果密文的安全不依赖于算法的保密，这种算法称为公开密码算法，如 DES、RSA 等；
- 数字签名：公开密钥算法的应用之一，用户可以采用自己的私钥对文件加以处理，由于私钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名；
- 数字信封：是公开密钥算法的应用之一，在数字信封中，公开密钥用来加密会话密钥（在加密消息时临时产生的，用来加密明文的对称算法的密钥，加密后即清零）；
- 数字证书：由用于标志通讯各方身份信息的一系列数据组成，一般由 CA 认证机构，即证书授权中心（Certificate Authority Center）发行。证书的国际标准有 X.509 与 SDSI；
- 密钥（key）：一个字符序列，公开密码算法中的加密或解密都依赖于它；用作加密时称加密密钥，用作解密时称解密密钥；
- 对称算法（symmetric algorithm）：又称传统密码算法，解密密钥能从加密密钥中推算出来的密码算法。大多数对称算法中，加解密密钥是相同的。这些算法也称单密钥算法。例如网盾中的"加密"功能就是单密钥算法的应用；
- 公开密钥算法（public-key algorithm）：又称非对称算法，用作加密的密钥不同于用作解密的密钥，而且在合理假定的长时间内解密密钥不能

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

根据加密密钥计算出来。用户要保障解密密钥的安全，而加密密钥则可以公开；

- 公开密钥（public key）：公开密钥算法中的加密密钥，简称公钥；
- 私人密钥（private key）：公开密钥算法中的解密密钥，简称私钥；
- 个人证书：可以理解为含有私钥的证书；
- 他人证书：可以理解为不含有私钥的证书；
- 摘要算法： 一种单向的算法，它对不定长度的数据进行计算，得出一定长度的计算结果，从这个结果无法反推出原始的数据。如果原始数据发生轻微的改变，则摘要结果就会发生重大改变，如果要改变原始数据的一部分而维持摘要不变是不可能的。同时，根据摘要产生另一条摘要与原始数据的摘要完全相同的数据也是不可能的。摘要算法的特性保证了如果数据在传输途中被破坏，无论这个破坏是有意的还是无意的，都一定能被检查出来；
- SHA-256 算法：一种优秀的摘要算法，它的计算结果为 256 位（32 个字节），而且具有非常快的计算速度，是公认的安全、有效的摘要算法。
- SM2 算法：SM2 算法作为一种高安全性、高效率的公钥密码算法，具备和 RSA 算法同样的加/解密、电子签名和密钥协商等重要的密码功能。
- 椭圆曲线公钥密码体制：新一代国产自主研发的公钥密码体制，具有最高的位安全强度，进一步加快了运算速度，缩短了数据传输的时间。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

2 产品概述

2.1 产品简介

格尔公钥基础设施产品，是格尔公司数字证书解决方案的基础平台。它包括格尔证书认证系统、证书注册系统、格尔密钥管理系统三个核心系统及证书状态在线查询系统、时间戳系统、证书综合服务系统、证书助手（PC 端和移动端）等基础平台支持设施，三个核心系统和诸多平台支持设施构成完整的、高效的认证体系架构，是一套成熟的、可靠的数字证书基础设施产品。

格尔电子证书系统在设计上符合国际通用标准，同时严格遵循国密办的各项规定，是一套开放式的系统，产品支持第三方 CA 系统、第三方 RA 系统的接入，也支持与第三方 KM 系统的对接。核心系统全部采用 JAVA 语言开发，具有良好的平台兼容性，可以支持 AIX、UNIX、Solaris、Linux、Windows 等操作平台，支持 Oracle、DB2、Sybase、MSSQL 等主流数据库和 Gbase、人大金仓、达梦等国产化数据库。系统设计灵活、可扩展性强，支持多级 CA 的分布式部署。

格尔电子证书系统针对不同的客户需求，将产品划分为三个系列：

- 格尔电子证书系统企业版；
- 格尔电子证书系统大客户版；
- 格尔电子证书系统运营中心版本。

企业版的证书设计容量为 1 万，适用于大中型企事业单位及中小企业用户，系统以硬件服务器的形式提供，也可以根据客户需求进行系统定制，由客户自行选择密码设备和数据库，具有部署快捷、操作简单、维护方便、管理简单等优点。

大客户版的证书设计容量为 1 万~10 万，面向政府部门、大型企业和金融机构等用户，提供完善的开发接口，可以应对客户的复杂需求，如接入其它第三方 CA 或 RA 系统等。

运营中心版主要提供给省级 CA，证书容量设计为千万级。

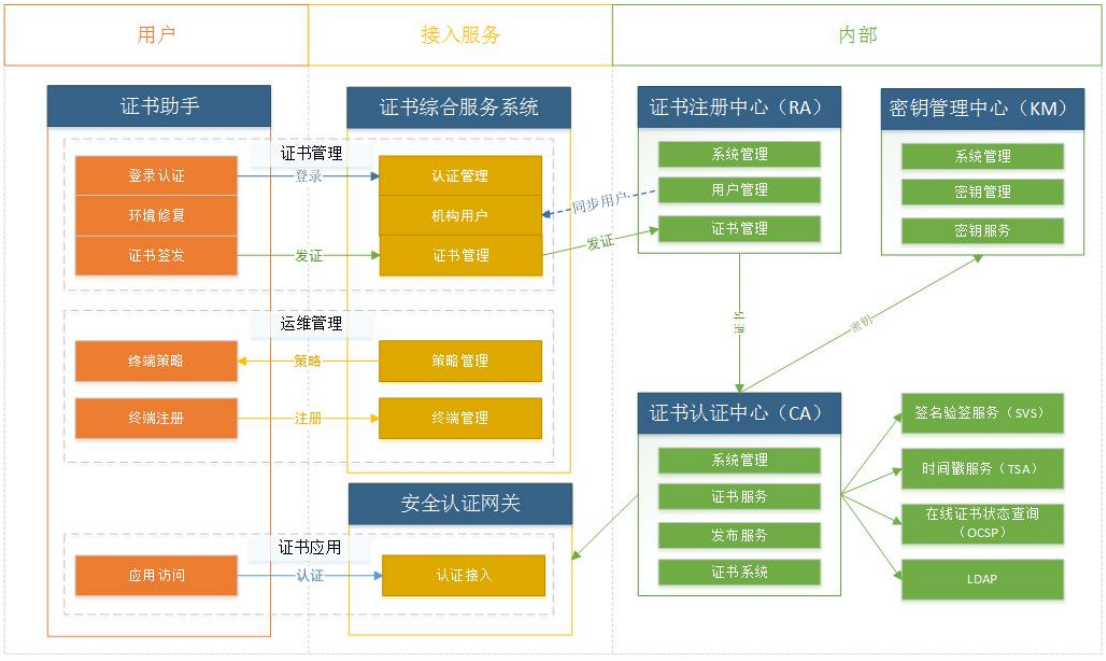
上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

2.2 产品组成

2.2.1 产品系统结构

格尔公钥基础设施由一系列软硬件实现模块组成，其核心包括七个模块：

- 格尔证书认证系统——CA
- 格尔证书注册系统——RA
- 格尔密钥管理系统——KM
- 格尔证书综合服务系统——CDS
- 格尔在线证书状态查询系统——OCSP
- 格尔时间戳管理系统——TSA
- 格尔证书助手——KCM



图表 1：系统结构图

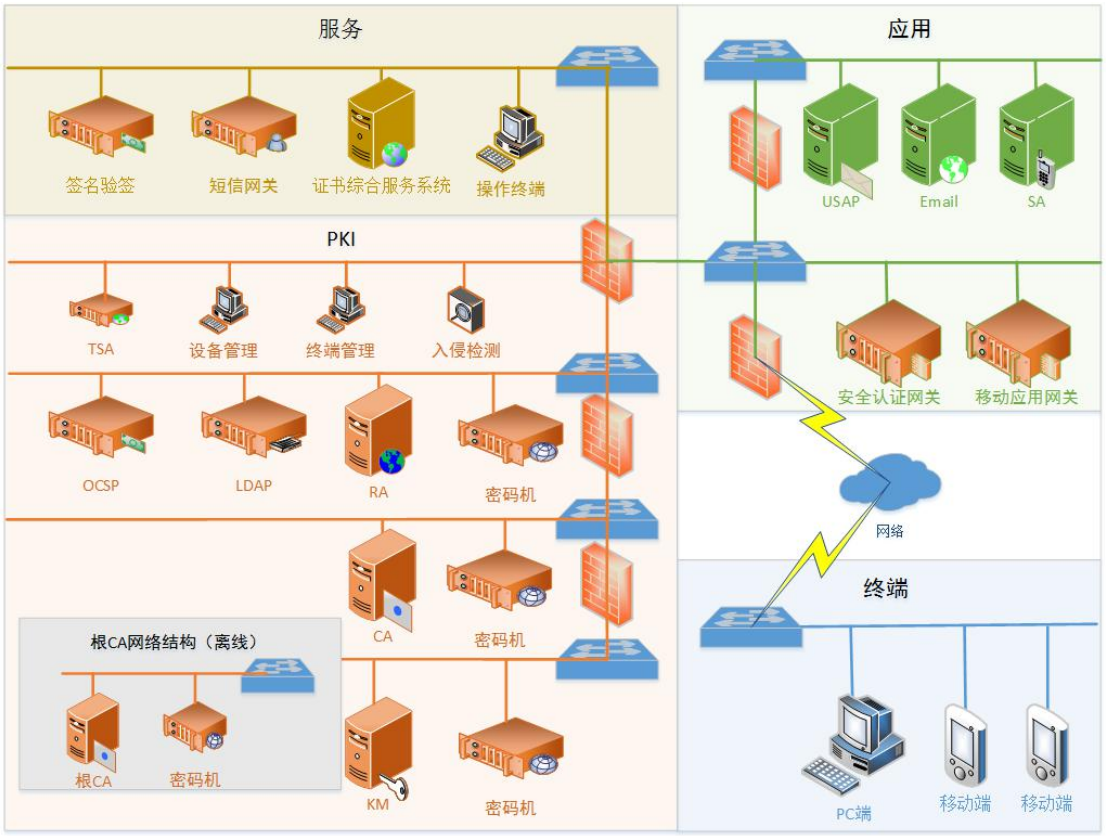
2.2.2 产品部署结构

产品面向的用户有内部用户和外部用户，对于外部用户（一般是移动端用户），则需要通过移动端证书助手进行证书发放，对于内部用户，可使用 PC 端证书助手进行发放。证书发放依赖于 PKI 证书服务（RA、CA、KM），证书服务

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

依赖于网关，对我的证书服务通过证书综合服务系统提供。

详细的网络示意图如下：



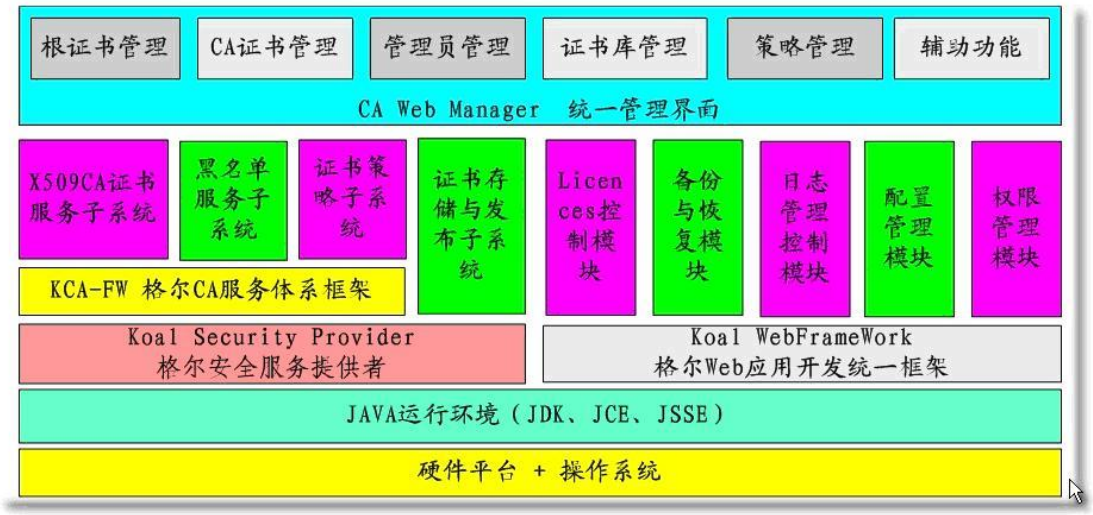
图表 2 应用示意图

2.2.3 格尔证书认证系统

CA 中心，又称为数字证书认证中心，作为电子商务交易中受信任的第三方，专门解决公钥体系中公钥的合法性问题。CA 中心为每个使用公开密钥的用户发放一个数字证书，数字证书的作用是证明证书中列出的用户名称与证书中列出的公开密钥相对应。CA 中心的数字签名使得攻击者不能伪造和篡改数字证书。

在数字证书认证的过程中，证书认证中心（CA）作为权威的、公正的、可信赖的第三方，其作用是至关重要的。认证中心就是一个负责发放和管理数字证书的权威机构。同样 CA 允许管理员撤销发放的数字证书，在证书废止列表(CRL)中添加新项并周期性地发布这一数字签名的 CRL。

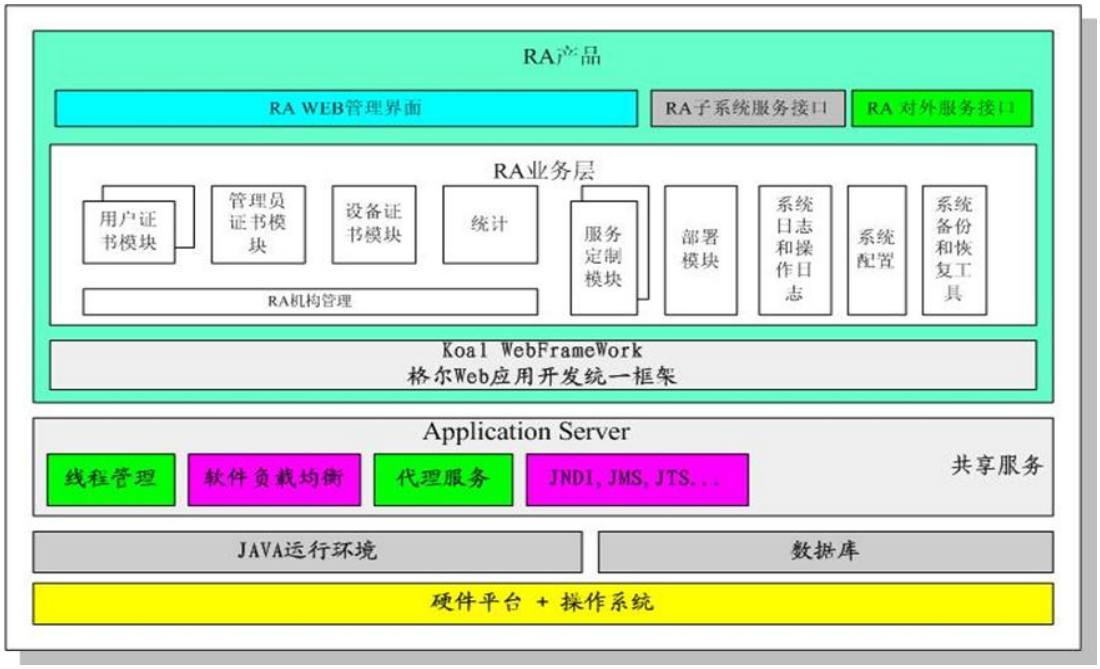
上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com



图表 3：格尔证书认证系统体系结构

2.2.4 格尔证书注册系统

RA（Registration Authority），数字证书注册审批机构。RA 系统是 CA 的证书发放、管理的延伸。它负责证书申请者的信息录入、审核以及证书发放等工作；同时，对发放的证书完成相应的管理功能。发放的数字证书可以存放于 IC 卡、硬盘或软盘等介质中。RA 系统是整个 CA 中心得以正常运营不可缺少的一部分。

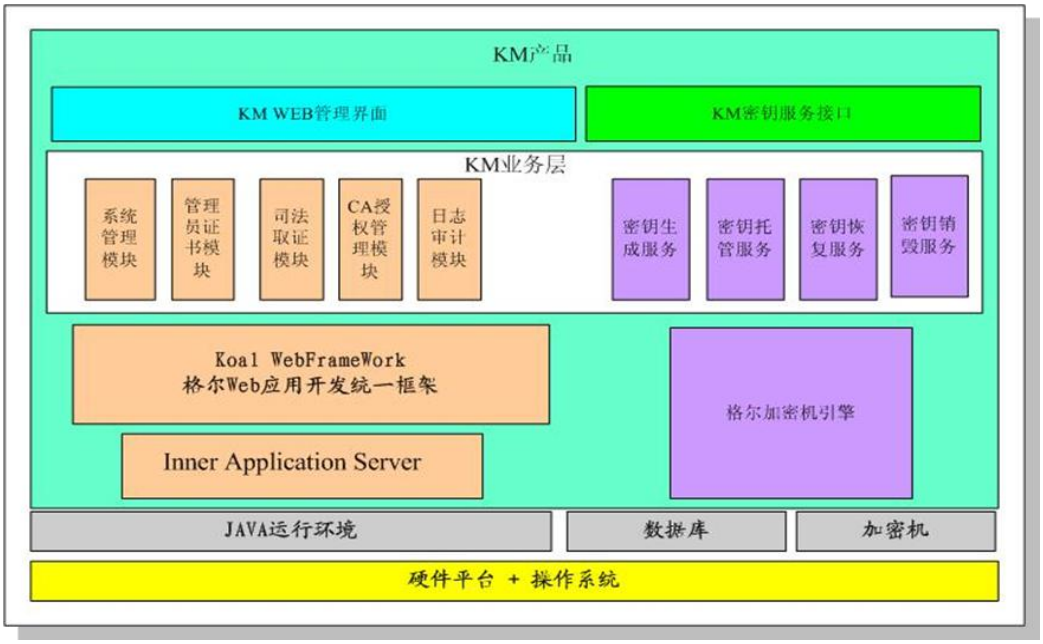


图表 4：格尔证书注册系统体系结构

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

2.2.5 格尔密钥管理系统

KM（Key Management），符合国密规范的密钥管理系统，它负责密钥的生成、恢复、安全存储和备份等，为 CA 提供密钥的生命周期管理服务。

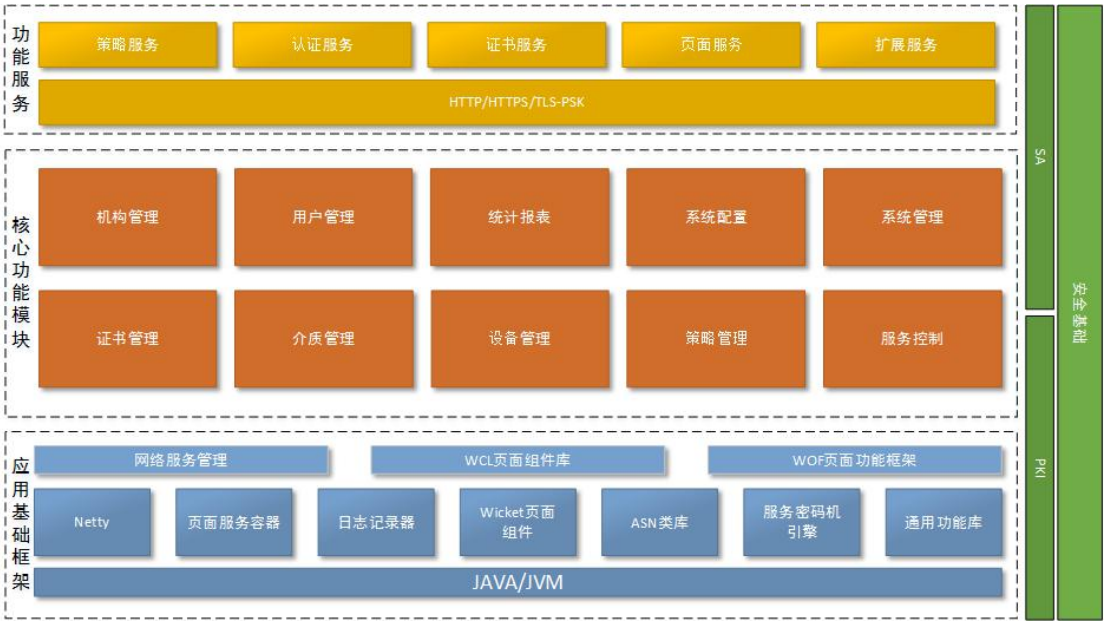


图表 5 格尔密钥管理系统体系结构

2.2.6 格尔证书综合服务系统

CDS 证书综合服务系统，提供对机构人员信息管理，认证服务，终端设备的管理，包含终端设备的安全使用、证书管理、接入管理、终端策略、发证策略等。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

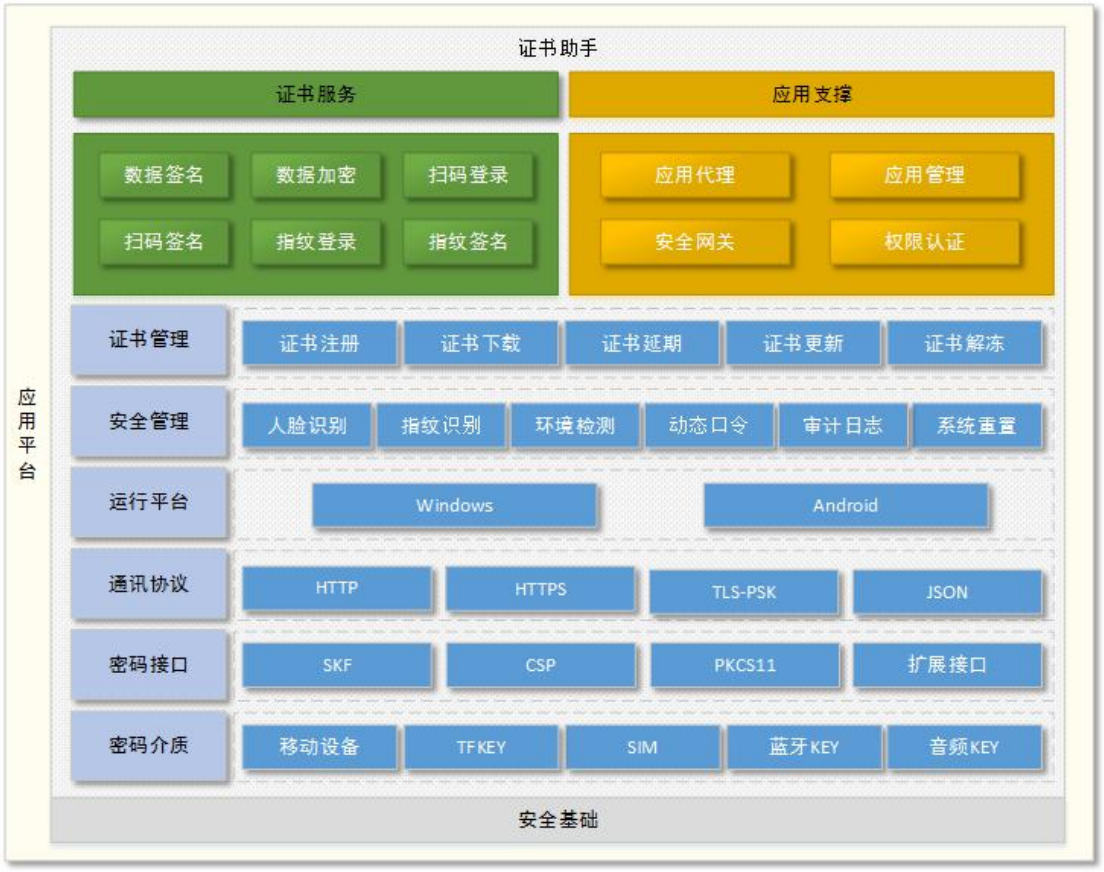


图表 6 证书综合服务系统体系结构

2.2.7 格尔证书助手

KCM 证书助手，支持 SM2 和 RSA 证书的发放，并支持证书的使用，通过对终端用户的身份确认，提供基于各种设备的证书签发、延期、废除，为个人用户提供证书的生命周期服务；并且支撑证书在终端的应用，配合安全认证网关提供基础的通讯认证服务。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com



图表 7 证书助手体系结构

图表 8 PC 端证书助手界面

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

图表 9 移动端证书助手界面

3 产品主要功能特点

3.1 基本特性

- 支持 CA 的树状信任模式，即系统可以支持 CA 多级扩展和多级认证；
- 支持 RSA 算法，密钥长度可达 2048 位；
- 全面支持国密 SM2 算法，密钥长度可达 256 位；
- 支持国密曲线 SM2 介质；
- 基于 B/S 结构的管理界面，内嵌 Web Sever，采用 https 安全远程管理机制进行安全登录；
- 支持签发电子邮件证书和对应的证书发布模式，可以使用 OutLook Express，OutLook，Foxmail 等进行电子邮件的加密和签名；
- 支持签发普通用户证书，SSL 客户端证书，机构证书，设备证书，VPN 证书；
- 支持移动端和 PC 端 SM2 证书的使用；
- 强大易用的部署向导帮助用户快速进行产品部署。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

3.2 高级特性

- 具有灵活的策略配置机制，可自定义证书策略；
- 支持 MofN 的安全登录机制；
- 支持管理与审计互相独立的二线三层的权限管理体系；
- 支持操作员权限按指定域、权限域、证书类型细分授权；
- 支持自定义证书有效期；
- 支持自定义证书延期有效时间；
- 支持证书自动归档；
- 基于 LDAP 的证书和 CRL 发布，CRL 发布采用了分块 CRL 与增量 CRL 技术；
- 支持基于 HTTP 的 CRL 发布；
- 支持直接使用 CSP 模式签发双证书，无缝接入新的证书介质；
- 支持基于 SSF33 算法的密钥不落地机制；
- 支持基于 SM1 算法的密钥不落地机制；
- 支持基于 SM4 算法的密钥不落地机制；
- 支持 SM1、SM4 对称算法、SM2 非对称算法、SM3 摘要算法；
- 支持多种签名算法，包括 RSA 证书支持 SHA1WithRSA、SHA256WithRSA，国密 SM2 证书支持 SM3WithSM2；
- 支持按照密钥类型独立运行、停止密钥生产服务；
- 大容量数据支持，在千万级数据下，界面查询翻页响应速度<5 秒。

3.3 兼容与扩展特性

- 支持 Windows10（向下兼容）、AIX、Solaris、Linux 等操作系统平台；
- 支持 Android4.4+平台；
- 支持 Iplanet Directory Server，IBM Directory Server，ITec Directory Server，Active Directory、Gbase 等多种 LDAP 发布系统；
- 支持 Oracle，DB2，Sybase，MySQL 等主流数据库和 Gbase、人大金仓、

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

达梦等国产化数据库；

- KM 支持接入第三方 CA 系统；
- CA 支持接入第三方 RA 系统，支持向上接入第三方 KM 系统；
- RA 支持接入第三方应用系统，支持两级 RA；
- 跨平台支持 SJY42、SJY15、SJL22、SJY42C、SHJ0901B、SJJ1012 等多种 RSA、SM2 加密机；
- 具备千万级以上的证书服务管理能力。

3.4 特别特性

- 支持签发微软的智能卡登录证书、域控制器证书、计算机证书，可以配置使用 ActiveDirectory 发布证书与黑名单，配合使用可以实现微软的智能卡登录，安全锁定工作站，因特网访问控制服务(IAS)；
- 支持双发布机制(同时发布到不同类型的 LDAP 目录)；
- 支持使用内嵌式数据搭建测试系统；
- 内嵌简易的用户密钥管理模块。
- 站点证书支持多域名；
- 支持审计报表；
- 支持批量发证以及其他证书业务操作；
- 支持超过 10000 个用户的单次批量注册；
- 支持多类型加密机配置，可以单独指定 RSA 加密机、SM2 加密机、管理根加密机及 SPKM 加密机。
- 支持 SCEP 协议直接对设备发放 RSA 或 SM2 双证书。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

4 产品参数

根据用户的需求不同，格尔证书认证产品划分成三个系列，分别提供不同级别的服务：

产品系列	证书容量
格尔电子证书系统企业版	1 万
格尔电子证书系统大客户版	1 万~10 万
格尔电子证书系统运营中心版	10 万~1000 万

图表 5 格尔公钥基础设施产品线划分

4.1.1 企业版

格尔企业版 CA 证书设计容量为 1 万张以下，主要面向大中型企事业单位及中小企业用户。格尔企业版 CA 是完整的 CA 系统，在系统结构上和大型 CA 完全一致，包括有证书注册模块、证书签发模块、证书发布模块、密钥管理模块等四个部分。

格尔企业版 CA 以一体化的硬件服务器形式提供（推荐模式），也可以根据客户需求进行系统定制。格尔企业版 CA 提供如下完备的证书管理功能：

- 用户信息注册/签发；
- 用户信息更新；
- 证书恢复；
- 证书废除；
- 证书重发；
- 微软智能卡证书/计算机证书/域控制器证书签发；
- 证书注销列表(CRL)与 CA 证书下载；
- 证书查询与发布。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

4.1.2 大客户版

大客户版 CA 的证书设计容量为 1 万~10 万，面向政府部门、大型企业和金融机构等用户，提供有完善的配套软件和开发接口，允许第三方的 CA 系统或 RA 系统接入。大客户版 CA 涵盖企业版 CA 的所有证书功能，同时提供以下高级特性：

- 分级 CA 管理；
- 证书策略管理；
- CRL 策略管理；
- 证书模板管理；
- RA 管理；
- 证书库统计。

4.1.3 运营中心版

专门针对证书运营中心建设，支持千万级的证书容量，产品通过国密局鉴定，具备最高的安全措施、管理审计机制和权限分配机制。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com

5 附录

5.1 SZT/SYT0901 数字证书认证系统资质

商用密码产品型号证书

（证书编号：SXH20147969 号）

单位名称：上海格尔软件股份有限公司

申报名称：基于国家密码标准算法的数字证书认证系统

批准型号：SZT0901 数字证书认证系统

说明：

证书有效期五年

国家密码管理局

2014 年 01 月 22 日

商用密码产品型号证书

（证书编号：SXH20147839 号）

单位名称：上海格尔软件股份有限公司

申报名称：非对称密钥管理系统

批准型号：SYT0801 密钥管理系统

说明：

证书有效期五年

国家密码管理局

2014 年 01 月 22 日

5.2 PKI 简介

数字认证信任技术主要是为网络信息空间提供一个信任的基准，即在用户实

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel：(86-021) 62327010 Fax：(86-021) 62327015
URL：http://www.koal.com

体和虚拟的网络空间中的用户角色之间建立一种映射关系，以便能将现实的物理世界中的信任关系移植到虚拟的网络空间中。

目前建立信任管理体系的关键技术主要是公钥基础设施 PKI 技术，该技术通过公钥密码体制中的用户私钥的机密性来提供用户身份的唯一性验证，并通过公钥数字证书的方式为每个合法用户的公钥提供一个合法性的证明，建立了用户公钥到证书 ID 号之间的唯一映射关系。数字证书中的信息通过数字信封技术和数字签名技术提供了完整性的保护，因此可以通过公开的方式（如 LDAP 服务）对外发布。

由于数字证书本身是公开的，因此在身份验证过程中必须通过公钥与私钥之间的唯一映射关系（由公钥加密体制自身提供保证）来间接建立用户私钥（用户身份）和证书 ID 号之间的映射关系。在统一的 PKI 信息安全平台实现中，用户的私钥是存放在实体鉴别密码器中的，因此私钥与用户身份之间的映射关系又多了实体鉴别密码器这一物理实体层的机制。

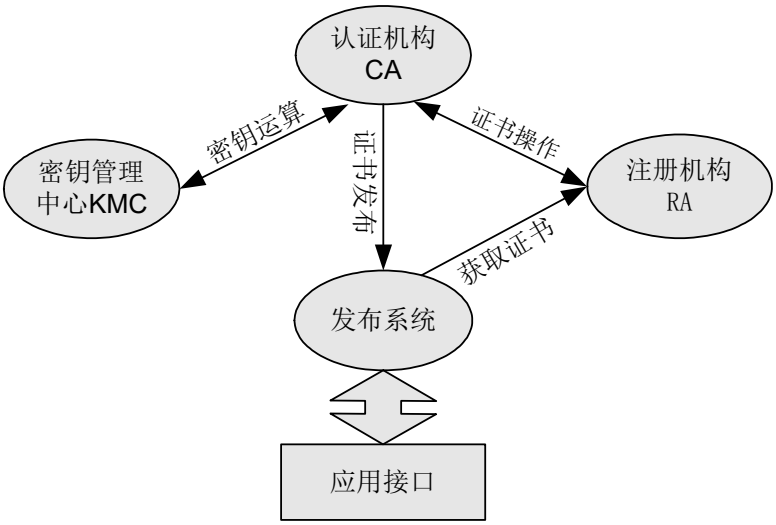
在多信任域的系统结构下，统一信任域内所颁发的数字证书将遵循相同的证书策略，而不同的信任域之间则可能存在策略上的差异。在进行跨信任域的信任验证操作时，必须首先就所使用的证书策略达成一致，才能保证多信任域体系结构所提供信任管理的一致性。

信任管理体系作为一种主流的第三方信任或公证管理体系已经在电子商务领域中得到了广泛的应用，而且已经进入正常服务运营的阶段。国外一些信息化程度较高的国家均已建立了完善的电子商务信任管理服务体系，面向一般公务员提供信任管理服务。

在典型的电子商务业务活动中，业务服务机构和各级机关人员通过信任管理服务体系相互验证对方的身份，并在此基础上完成最终的业务处理。由于电子商务在全球范围内（尤其是发达国家）的普及和推广，应该可以认为 PKI 技术的合理性和可行性已经得到了充分的验证和说明。

通常情况下，PKI 数字认证系统建设由密钥管理中心 KMC、证书认证中心（CA）、证书注册审核中心（RA）、证书/CRL 发布及查询系统以及和应用系统间的接口五部分组成，其功能结构如下图所示：

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com



图表 11 PKI 数字认证中心功能结构

密钥管理中心（KMC）：是公钥基础设施中的一个重要组成部分，负责为 CA 系统提供密钥的生成、保存、备份、更新、恢复、查询等密钥服务，以解决分布式企业应用环境中大规模密码技术应用所带来的密钥管理问题。

认证中心（CA）系统：CA 认证中心是 PKI 公钥基础设施的核心，它主要完成生成/签发证书、生成/签发证书撤销列表（CRL）、发布证书和 CRL 到目录服务器、维护证书数据库和审计日志库等功能。

注册中心（RA）系统：RA 注册中心是数字证书的申请、审核和注册的机构。它是 CA 认证中心的延伸，在逻辑上 RA 和 CA 是一个整体，主要负责提供证书注册、审核以及发证功能。

证书发布与查询服务系统：证书发布与查询系统主要提供 LDAP 服务、OCSP 服务和注册服务。注册服务为用户提供在线注册的功能；LDAP 提供证书和 CRL 的目录浏览服务；OCSP 提供证书状态在线查询服务。

系统应用接口：系统应用接口为外界提供使用 PKI 安全服务的入口。系统应用接口一般采用 API、JavaBean、COM 等多种形式。

以上五部分之间的配合协作，对外提供 PKI 信任基础设施的安全服务。

上海格尔软件股份有限公司/上海格尔安全科技有限公司
上海市静安区江场西路 299 弄中环时代广场 4 号楼 6 楼 Tel: (86-021) 62327010 Fax: (86-021) 62327015
URL: http://www.koal.com