商用密码产品介绍

主讲人：朱勋

天津市商用密码行业协会

目录

CONTENTS

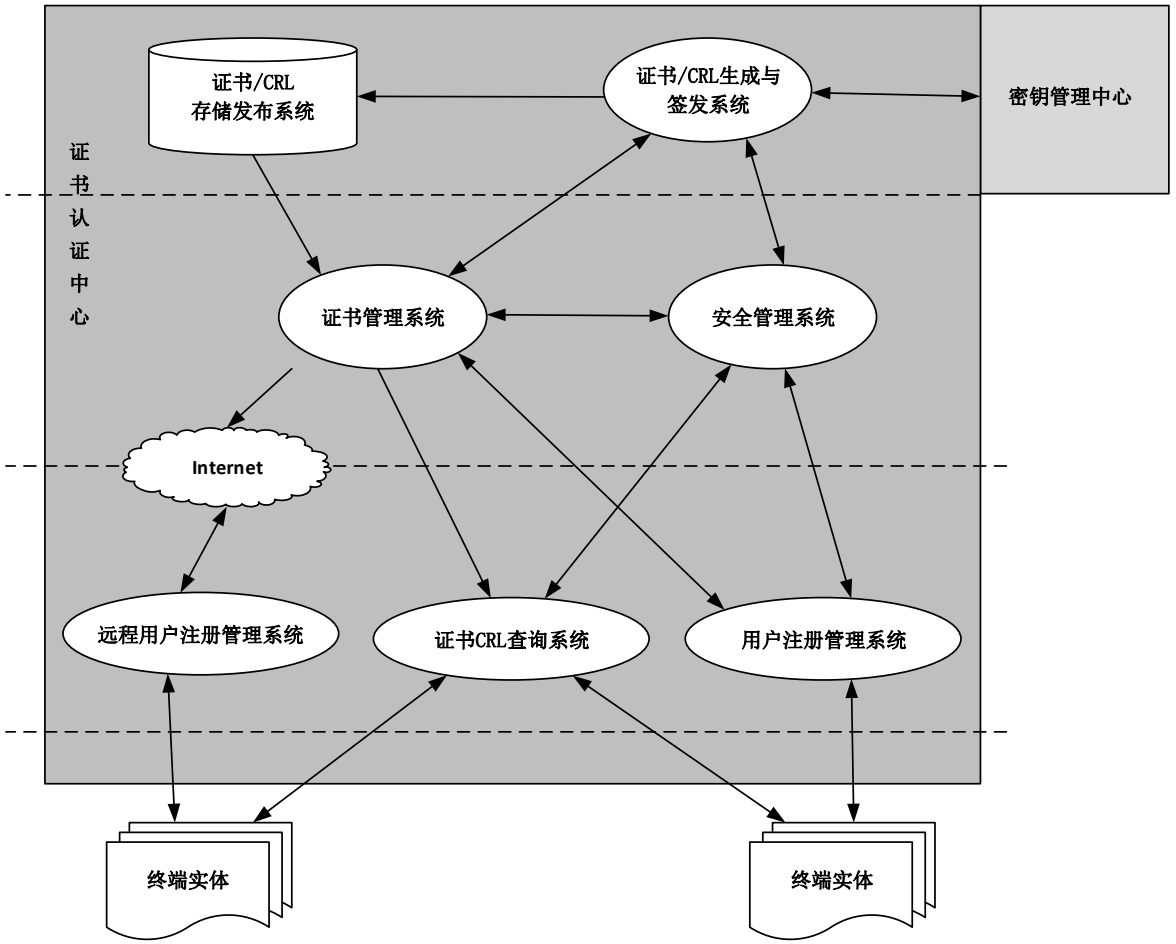
数字证书认证系统

PART. 01

1.1系统介绍

对生命周期内的数字生疏进行全过程管理的安全系统，数字证书认证系统必须采用双证书（签名和加密证书）机制，并按要求建设双中心(证书认证中心和密钥管理中心)。逻辑上可分为核心层、管理层和服务层，其中核心层由密钥管理中心、证书/CRL生成与签发系统、证书/CRL 存储发布系统构成；管理层由证书管理系统和安

全管理系统构成；服务层由证书注册管理系统和证书查询系统构成。



1.2功能介绍

- CA主要功能：

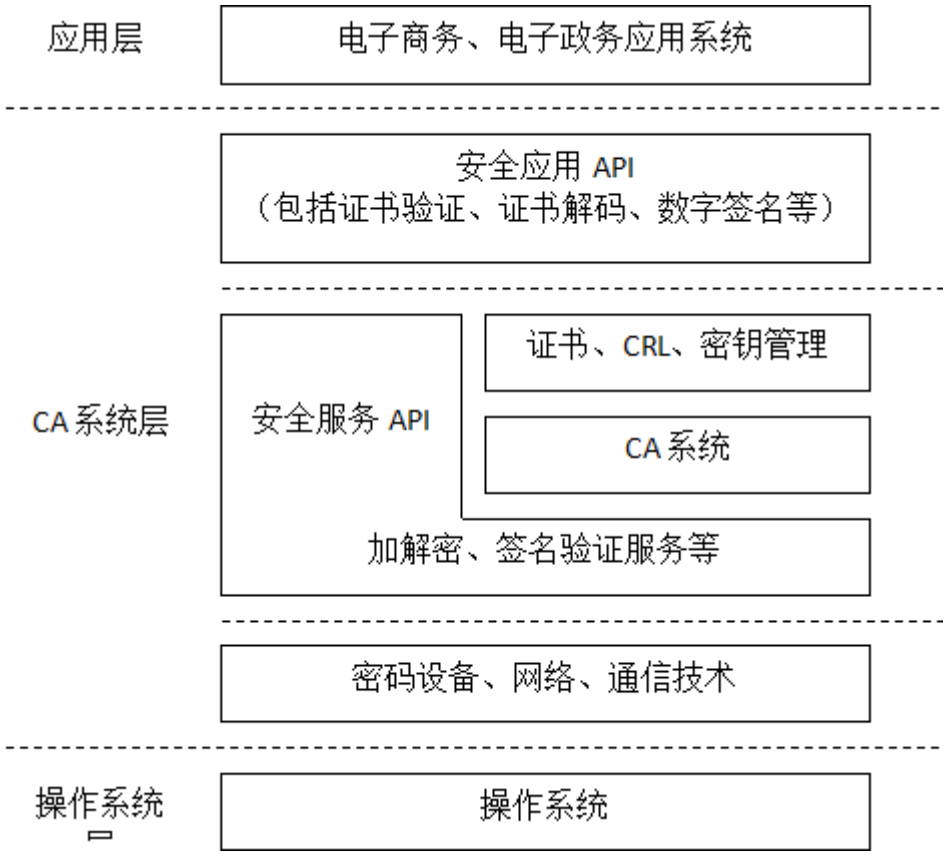
1.提供数字证书在其生命周期中的管理服务
2.提供RA的多种建设方式：RA可全部托管在CA，也可部分托管在CA，远端部署
3.提供人工审核或自动审核两种审核模式
4.支持多级CA:提供证书签发、证书查询、证书状态查询、CRL下载、目录服务等

- RA主要功能：负责用户证书申请、身份审核和证书下载，可分为本地注册管理系统和远程注册管理系统

证书申请和下载均可采用在线和离线方式，包括用户信息的录入、审核、证书下载、安全审计、安全管理
及多级审核

- KM功能包括：生成非对称密钥对、对称密钥、用于前程过程的随机数；接收、审核CA的密钥申请；调用备用库中的密钥对，向CA发送密钥对等，一般与密码机直接，密钥由服务器密码机产生。
提供了对生命周期内的加密证书密钥对进行全过程管理管理功能，包括密钥生成、储存、备份、更新撤销、归档、恢复等。

1.3技术架构

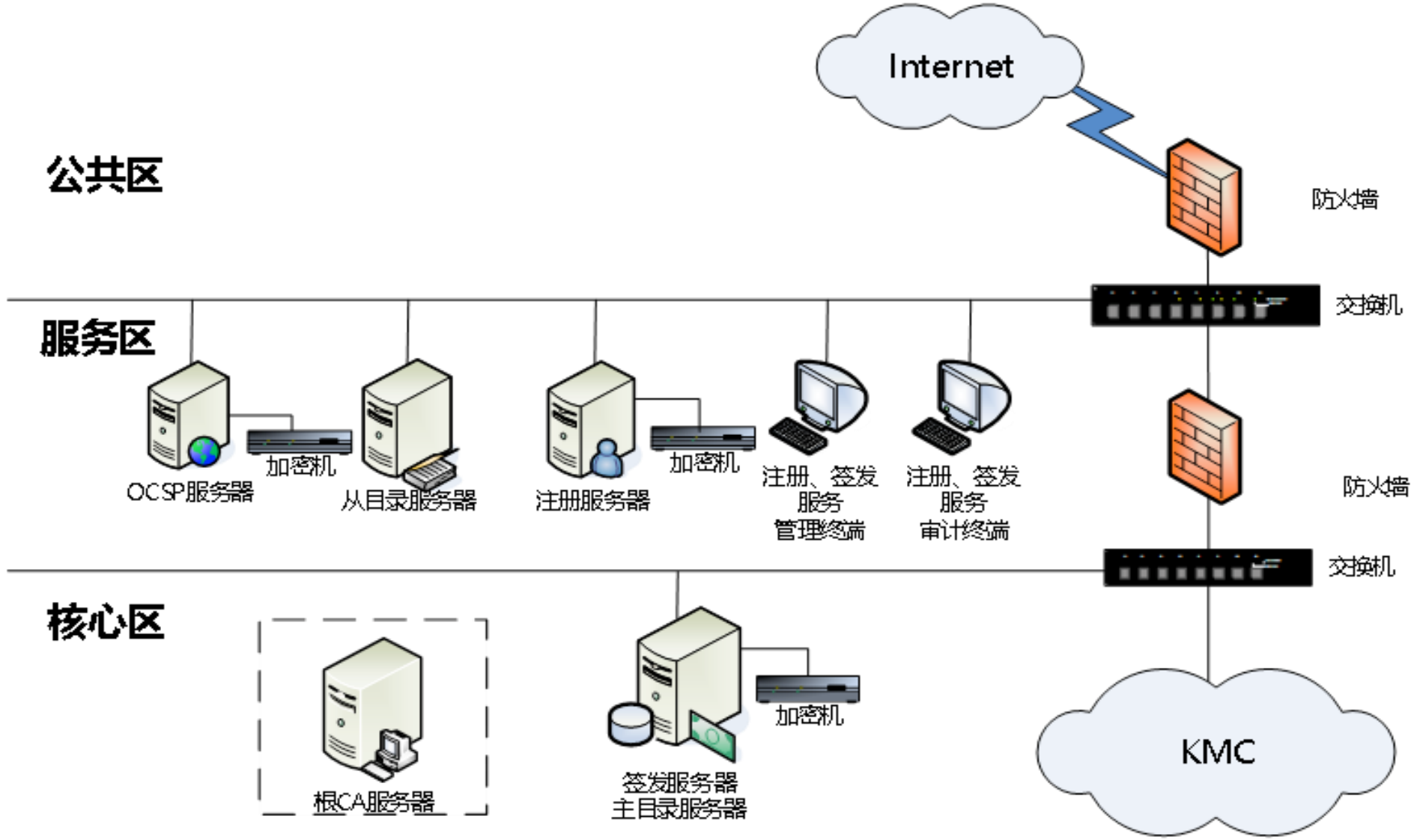


灵创智恒数字证书管理系统体系为三级架构：最底层位于操作系统之上，为密码技术（包括密码设备）、网络技术、通信技术等；中间层为安全服务API和CA服务，以及证书、CRL和密钥管理服务；最高层为安全应用API，包括证书验证、证书解码、数字信封、基于证书的数字签名和身份认证等API，为上层的各种电子商务、电子政务应用提供标准的接口

1.4技术标准

GM/T 0015-2012 基于SM2密码算法的数字证书格式规范
GM/T 0010-2012 SM2密码算法加密签名消息语法规范
GM/T 0034-2014基于SM2密码算法的证书认证系统密码及其相关安全技术规范
GM/T 0014-2012 数字证书认证系统密码协议规范
GM/T 0038-2014 证书认证密钥管理系统检测规范
GM/T 0037-2014证书认证系统检测规范
GB/T 16264.8-2005 信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架
GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式
PKCS系列标准
PKIX系列标准
LDAP V3协议
OCSP协议
SSL/TLS协议

1.3产品部署


Internet
公共区
防火墙
交换机
服务区
OCSP服务器
加密机
从目录服务器
注册服务器
加密机
注册、签发
服务
管理终端
注册、签发
服务
审计终端
防火墙
交换机
核心区
根CA服务器
加密机
签发服务器
主目录服务器
KMC

密钥管理系统

PART. 02

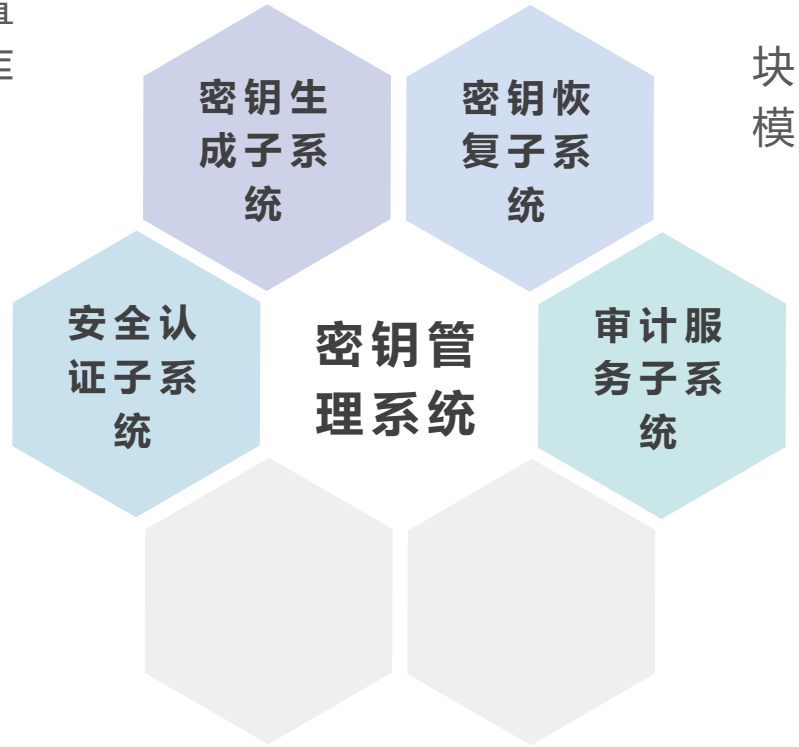
2.1系统介绍

密钥管理系统其主要功能是实现用户加密密钥的生成、存储、分发、更新、归档、销毁等全生命周期的管理。密钥管理系统支持多种主流的加密设备（多种密码卡，密码服务器），支持RSA和SM2公钥密码算法，系统能够同时为多个CA系统提供密钥管理服务。

2.2系统组成

密钥生成系统是由系统配置模块、密钥生成模块、数据库组件组成。

密钥恢复系统由系统配置模块、密钥查询模块、密钥恢复模块组成。



安全认证子系统是由系统配置模块、用户管理模块、CA机构管理模块、安全认证模块和数据库组件组成。

审计服务子系统由审计接口、审计服务模块和数据库组件构成。

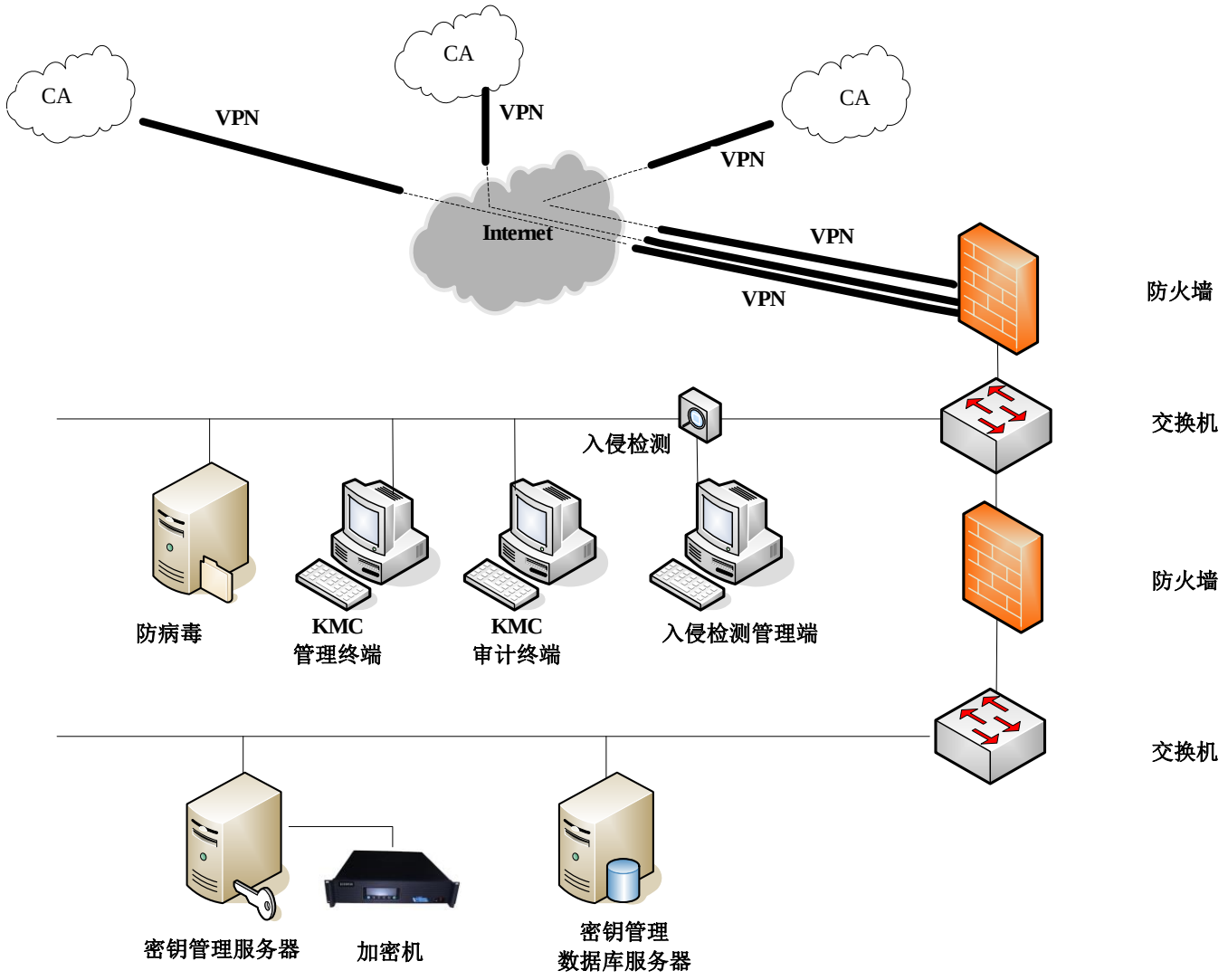
2.3密钥管理

名称	生成	存储	分发	备份	更新	撤销	归档	恢复
加密密钥对	根据CA的请求为用户生成非对称密钥对，由密管中心硬件设备生成	加密存储在数据库中	通过证书认证系统分发到用户证书载体中	热备份、冷部分、异地备份	生成新的非对称密钥对	根据CA请求撤销当前使用的密钥	对到期或撤销的密钥提供安全长期的存储	为用户提供密钥恢复，为司法取证提供特定密钥恢复

2.4标准规范

- GM/T 0015-2012 基于SM2密码算法的数字证书格式规范
- GM/T 0010-2012 SM2密码算法加密签名消息语法规范
- GM/T 0034-2014基于SM2密码算法的证书认证系统密码及其相关安全技术规范
- GM/T 0014-2012 数字证书认证系统密码协议规范
- GM/T 0038-2014 证书认证密钥管理系统检测规范
- GM/T 0037-2014证书认证系统检测规范
- GB/T 16264.8-2005 信息技术 开放系统互连 目录 第8部分：公钥和属性证书框架
- GB/T 20518-2006 信息安全技术 公钥基础设施 数字证书格式
- PKCS系列标准
- PKIX系列标准

2.5产品部署


CA
CA
CA
VPN
VPN
VPN
Internet
VPN
VPN
防火墙
交换机
入侵检测
防病毒
KMC
管理终端
KMC
审计终端
入侵检测管理端
防火墙
交换机
密钥管理服务器
加密机
密钥管理
数据库服务器

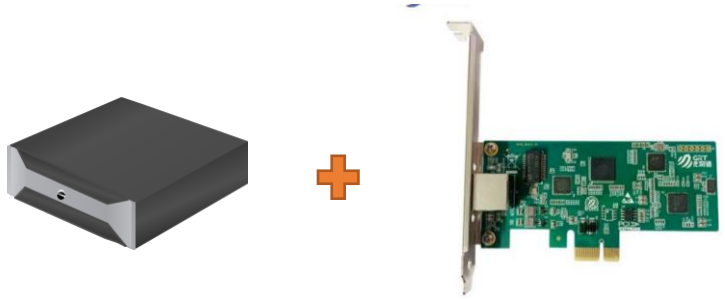
签名验签服务器

PART. 03

3.1 产品介绍

➢签名验签服务器

特点：
- 基于PKI体用和数字证书的数字签名、验签技术
- 对应用系统接口通用，易开发
- 关键业务信息的真实性、完整性和不可否认性



实现方式：对密码卡进一步封装

三种服务方式：

1.API调用方式，业务系统通过GM /T -0020-2012 《证书应用综合服务接口规范》中规定的API访问签名验签服务器

签名验签服务器是为应用实体提供基于PKI体系和数字证书的数字签名、验证签名的运算功能服务器可以保证关键业务信息的真实性、完整性和不可否认性，主要用于数字证书认证系统、电子银行、电子商务、电子政务等基于PKI的业务系统，为这类业务系统提供数字证书管理和验证服务。

3.2通信标准

2.通用请求方式: 通过GM/T 0029-2014 附录A中规定的协议，请求者将数字签名、验证数字签名等请求发给签名验签服务器完成签名验签服务并返回结果。(ASN.1)

3.HTTP请求响应方式：由ASN.1格式转换为HTTP协议中的文本格式，通过HTTP请求发送给签名验签服务器

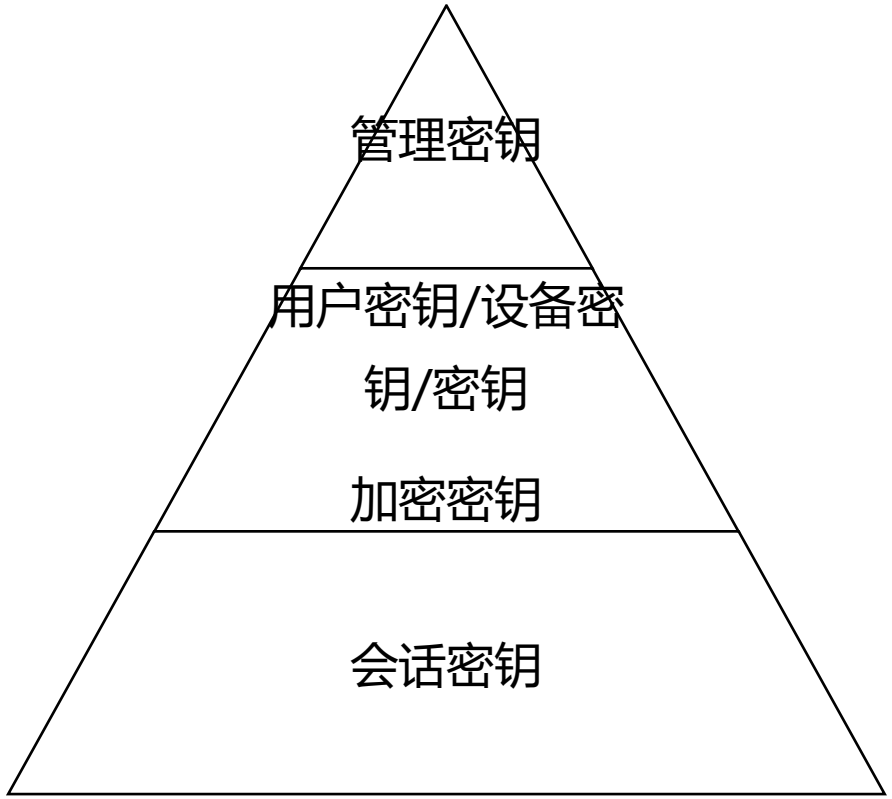
ASN.1

```
SVSRequest ::= SEQUENCE {
version                    Version DEFAULT v1,
reqType                    ReqType,
request                    Request,
reqTime                    GeneralizedTime
}
```

HTTP

```
POST /SignDataHTTP/1.1\r\n
SVS-Request-Version：v1\r\n
SVS-Request-Time：20131001120000Z+0800\r\n
Content-Type：application/x-www-form-urlencoded\r\n
Content-Length：实际请求 body 长度\r\n
\r\n
signMethod=…
```

3.3密钥体系

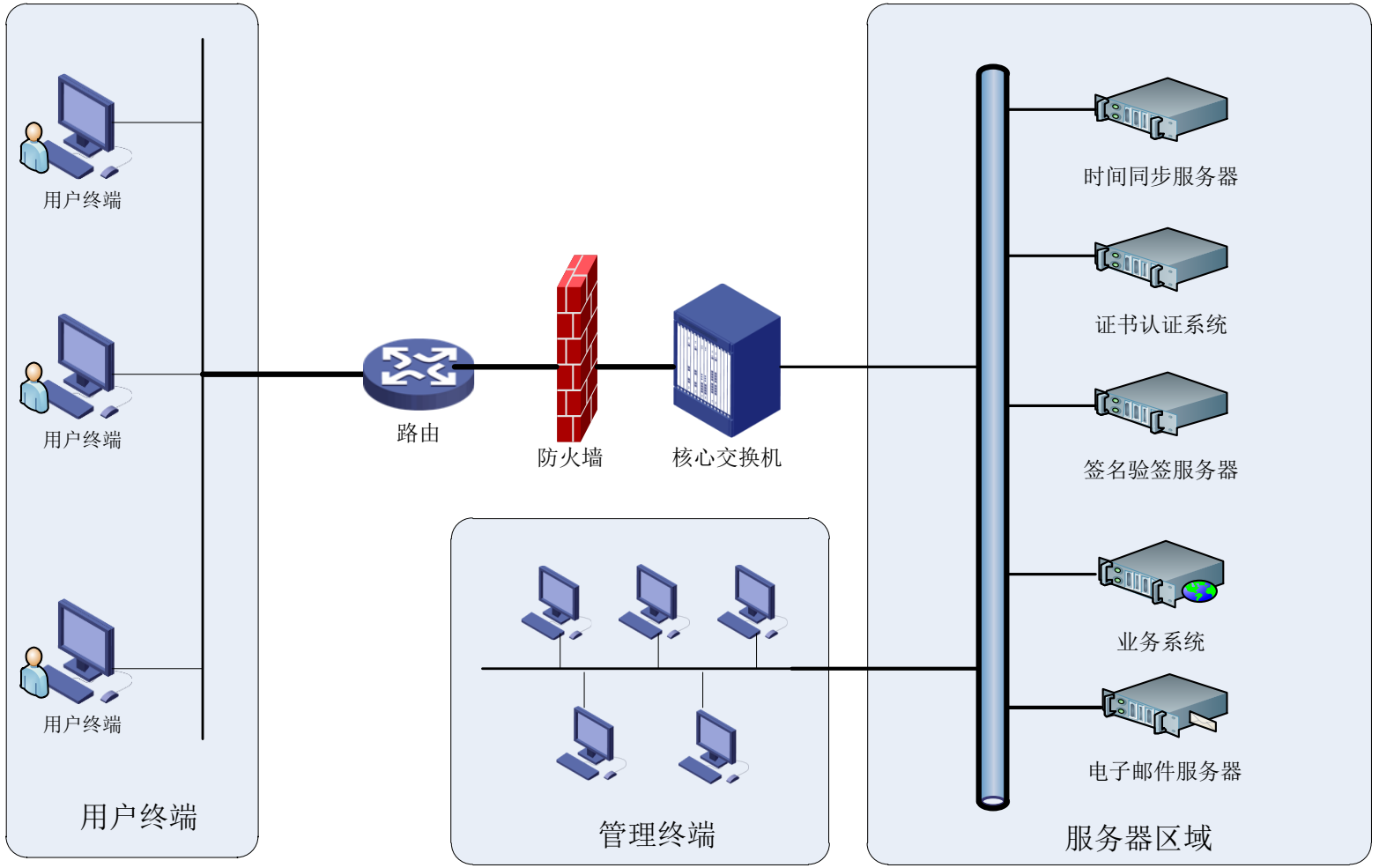


名称	作用
管理密钥	保护服务器密码机中密钥和敏感信息的安全密钥管理员密钥、通道密钥、完整性密钥、
用户密钥	用户的身份密钥，包括签名和加密密钥对，签名密钥由服务器密码机产生，用于实现用户签名、验证、身份鉴别等。加密密钥对由KM系统产生，对会话密钥和数据进行加解密。
设备密钥	设备密钥是服务器密码机的身份密钥，用于设备管理 密钥生成方式和用户密钥相同
密钥加密密钥	定期更换的对称密钥，对产生的会话密钥保护
会话密钥	对称密钥，用于数据加解密，需采用数字信息进行导出/导入

3.4标准规范

- GM/T 0002-2012 SM4分组密码算法
- GM/T 0029-2014 签名验签服务器技术规范
- GM/T 0028-2014 密码模块安全技术要求
- GM/T 0039-2015 密码模块安全检测要求
- GM/T 0004-2012 SM3密码杂凑算法
- GM/T 0006-2012 密码应用标识规范
- GM/T 0009-2012 SM2密码算法使用规范
- GM/T 0010-2012 SM2密码算法加密签名消息语法规范

3.5系统部署


用户终端
用户终端
用户终端
用户终端
路由
防火墙
核心交换机
管理终端
时间同步服务器
证书认证系统
签名验签服务器
业务系统
电子邮件服务器
服务器区域

安全认证网关

PART. 04

4.1产品简介

安全认证网关是采用数字证书技术为应用系统提供用户管理、身份鉴别、单点登录、传输加密、访问控制和安全审计服务等功能产品，保证了网络资源的的安全访问。与一般网关产品的主要区别是采用了数字证书技术。安全网关可分为代理模式和调用模式。安全网关基于IPSEC /SSL VPN 协议实现。

4.2产品组成

能对需要访问系统相关用户进行增删改查；支持角色管理、支持从第三方平台同步用户信息

证书管理模块主要包括证书查询、用户证书管理等功能。

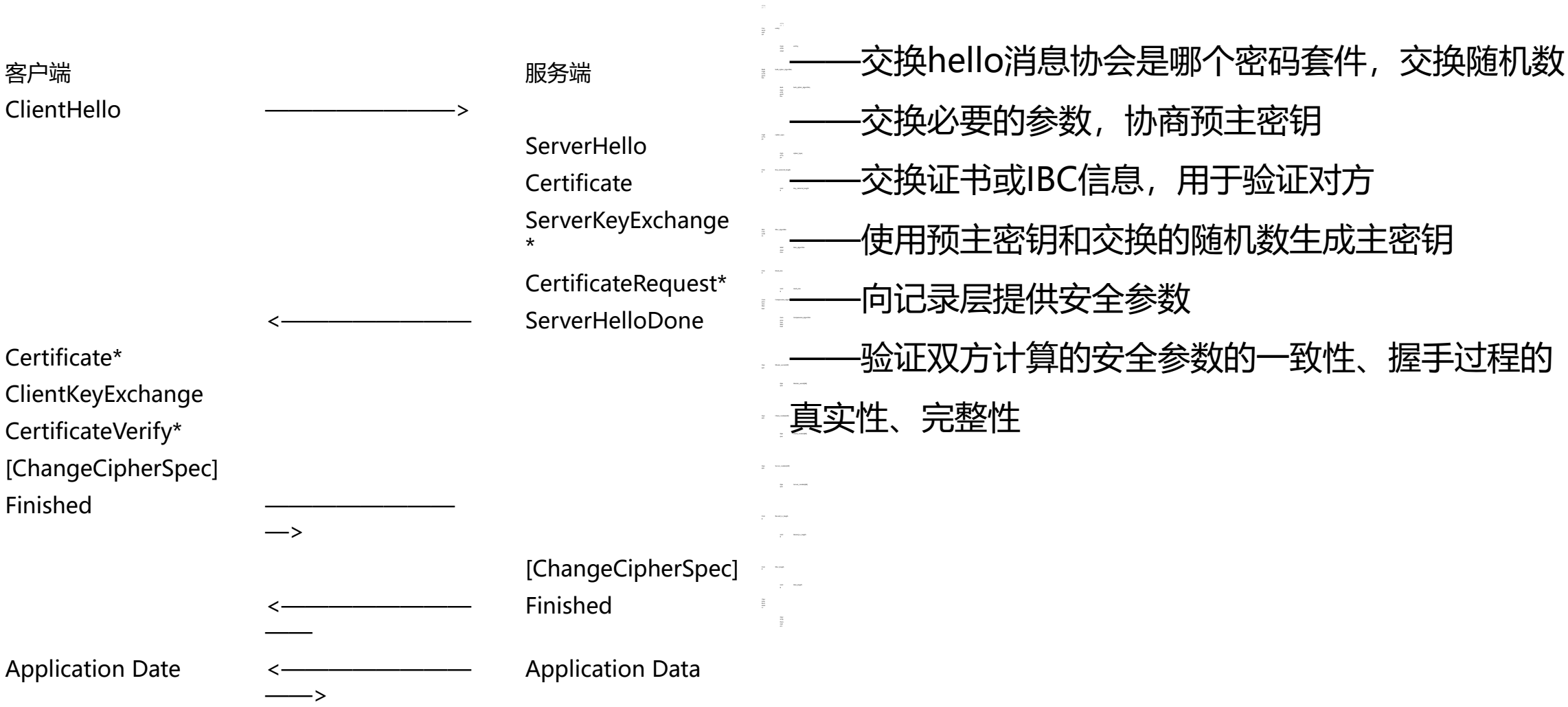
支持网段、TCP/UDP及端口号应用系统
支持WEB应用：按照协议(http/https)、域名、端口号、WEB标识进行识别

持基于数字证书的身份鉴别
单双向SSL认证:支持设置是否需要用户提交数字证书

支持对单个用户或角色访问应用的权限进行增删改查
支持黑白名单模式
支持权限最小化模型

对用户对系统的访问进行详细记录，记录信息包括：时间、用户IP、用户证书信息、事件类型、访问资源、上传流量、下载流量、访问结果、错误原因、成功和失败标识

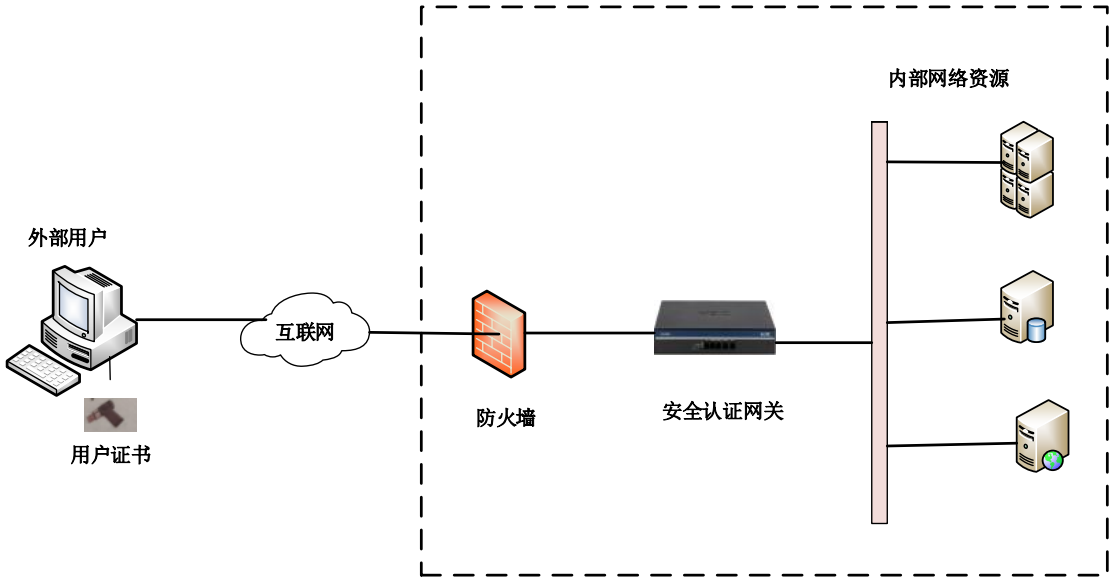
4.3握手协议

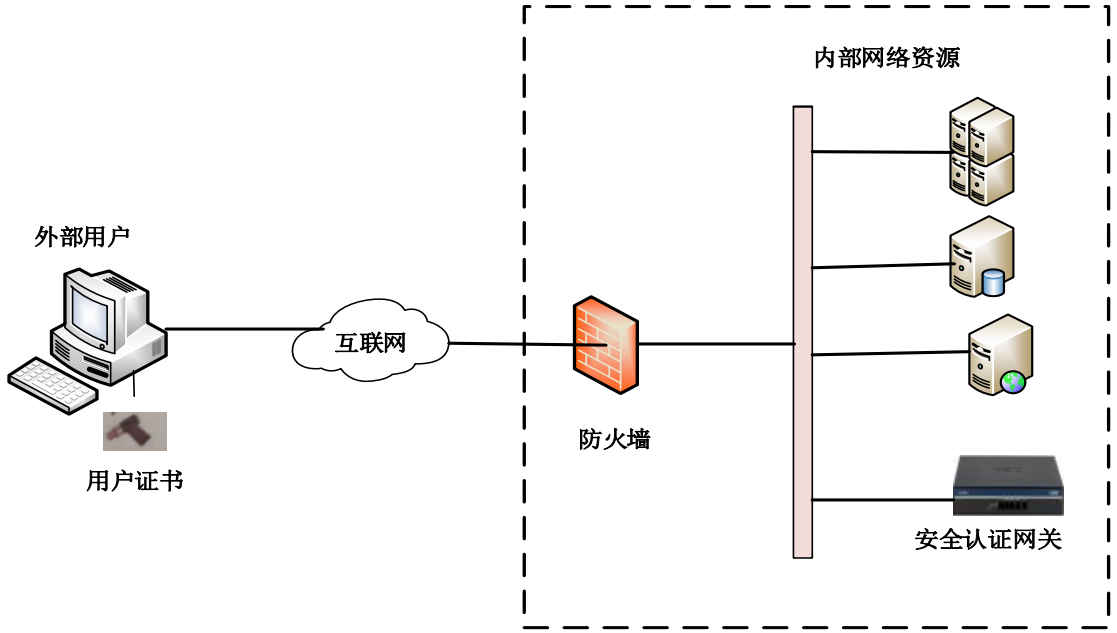

客户端
服务端
ClientHello
ServerHello
Certificate
ServerKeyExchange*
CertificateRequest*
ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished
[ChangeCipherSpec]
Finished
Application Date
Application Data
——交换hello消息协会是哪个密码套件，交换随机数
——交换必要的参数，协商预主密钥
——交换证书或IBC信息，用于验证对方
——使用预主密钥和交换的随机数生成主密钥
——向记录层提供安全参数
——验证双方计算的安全参数的一致性、握手过程的真实性、完整性

4. 4 标准规范

- GM/T 0005-2012 随机性检测规范;
- GM/T 0003-2012 SM2椭圆曲线公钥密码算法 ;
- GM/T 0004-2012 SM3密码杂凑算法;
- GM/T 0002-2012 SM4分组密码算法;
- GM/T 0009-2012 SM2密码算法使用规范;
- GM/T 0010-2012 SM2密码算法加密签名消息语法规范;
- GM/T 0015-2012 基于SM2密码算法的数字证书格式规范;
- GM/T 0014-2012 数字证书认证系统密码协议规范;
- GM/T 0024 -2014 SSL VPN 技术规范
- GM/T 0026-2014 安全认证网关产品规范;
- GM/T 0006-2012 密码应用标识规范;
- GB/T 9813 微型计算机通用规范
- PKCS系列标准
- PKIX系列标准

4. 5产品部署





物理串联：用户必须经过网关才能访问到受保护的应用

可以由应用或者防火墙进行逻辑判断，识别未经过网关的IP，实现逻辑串联

感谢聆听

天津市商用密码行业协会