GM/T 0024-2014
SSL VPN技术规范

宣讲人 罗俊

2014年7月24日

目录

- 标准的适用范围和作用
- 标准的编制思路和技术路线
- 标准的主要内容解读
- 标准应用时的注意事项
- 应用举例

目录

标准的适用范围和作用

- 适用范围
  - 对SSL VPN的技术协议、产品的功能、性能和管理以及检测进行了规定
  - 用于指导SSL VPN产品的研制、检测、使用和管理
- 作用
  - 统一SSL VPN产品的协议规范和技术要求
  - 规范商用密码算法在SSL VPN产品的使用
  - 为不同厂家SSL VPN产品的互联互通提供标准

目录

- 标准的适用范围和作用
- 标准的编制思路和技术路线
- 标准的主要内容解读
- 标准应用时的注意事项
- 应用举例

标准的编制思路和技术路线

- 编制思路
  - 通用性：统一技术要求，实现基本技术规格一致
  - 灵活性：对管理方式、硬件配置等不做细节规定
  - 安全性：硬件、软件、管理安全性都有严格规定
- 技术路线
  - 支持我国自主研制的商用密码算法
  - 参照TLSv1.1协议，引入双证书体制
  - 增加基于ECC和IBC的认证模式和密钥交换模式
  - 强化安全性，取消DH密钥交换方法
  - 增加网关到网关协议部分，规范SSL隧道

标准的编制思路和技术路线

- 2008年启动本标准编制，2012年进行修订
- 由联合课题组承担编制工作
- 经多方、多轮征意、修改及评审
- 于2014年正式发布，标准号GM/T0024-2014

目录

标准的主要内容解读

- 本规范共分为9个章节
  - 1、范围
  - 2、规范性引用文件
  - 3、术语与定义
  - 4、符号和缩略语
  - 5、密码算法与密钥种类
  - 6、协议
  - 7、产品要求
  - 8、产品检测
  - 9、合格判定

标准的主要内容解读密码算法

- 非对称算法：
  - SM2椭圆曲线密码算法
  - 2048位及以上的RSA算法
    - SM9（IBC）算法
- 对称密码算法
  - SM1分组密码算法
  - SM4分组密码算法
  - CBC(分组链接)模式
- 密码杂凑算法使用SM3或SHA-1算法

标准的主要内容解读密码算法

- 数据扩展函数

A(0)=seed，A(i)= HMAC(secret, A(i-1))；

P_hash(secret，seed)=HMAC(secret, A(1)+seed)+
HMAC(secret, A(2)+seed)+
HMAC(secret, A(3)+seed)+…

消息摘要算法（SM3）

密钥

数据

可反复迭代直至产生要求长度的数据

- 伪随机函数PRF

PRF (secret,label,seed) =P_SM3(secret,label+seed)

标准的主要内容解读 密钥种类

- **密钥种类**
  - **服务端密钥**
    - 签名密钥对
    - 加密密钥对
  - **客户端密钥**
    - 签名密钥对
    - 加密密钥对

通过CA向密钥管理中心申请

VPN自身密码模块产生

预主密钥

主密钥

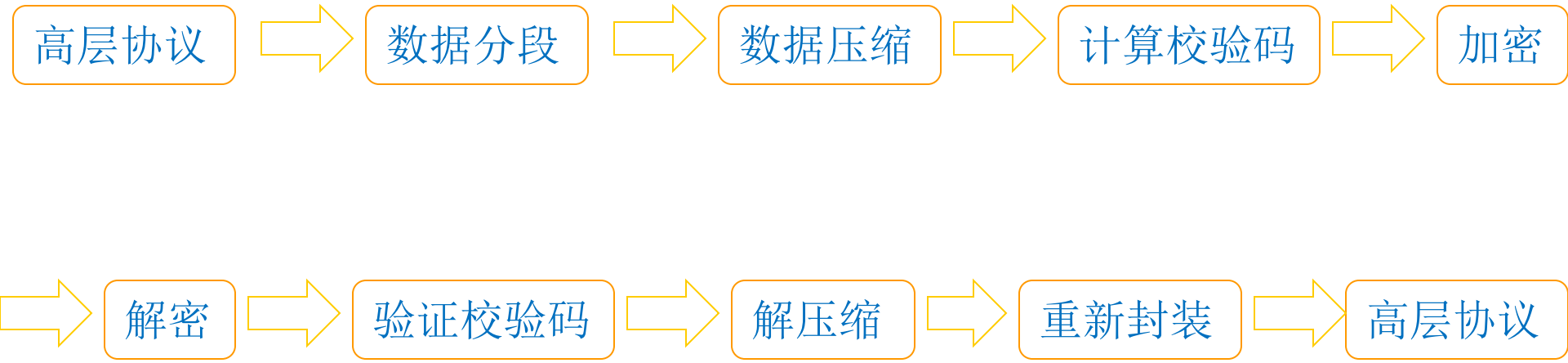
PRF(pre_master_secret, "master secret“, server_random +client_random) [0..47]

工作密钥

- 客户端写校验密钥 保护客户端发送数据的完整性
- 服务端写校验密钥 保护服务端发送数据的完整性
- 客户端写密钥 保护客户端发送数据的机密性
- 服务端写密钥 保护服务端发送数据的机密性

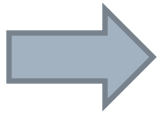
PRF(master_secret, "key expansion", server_random +client_random);

标准的主要内容解读 记录层协议



标准的主要内容解读 握手协议

安全会话
会话标识
数字证书
压缩方法
密码规格
主密钥

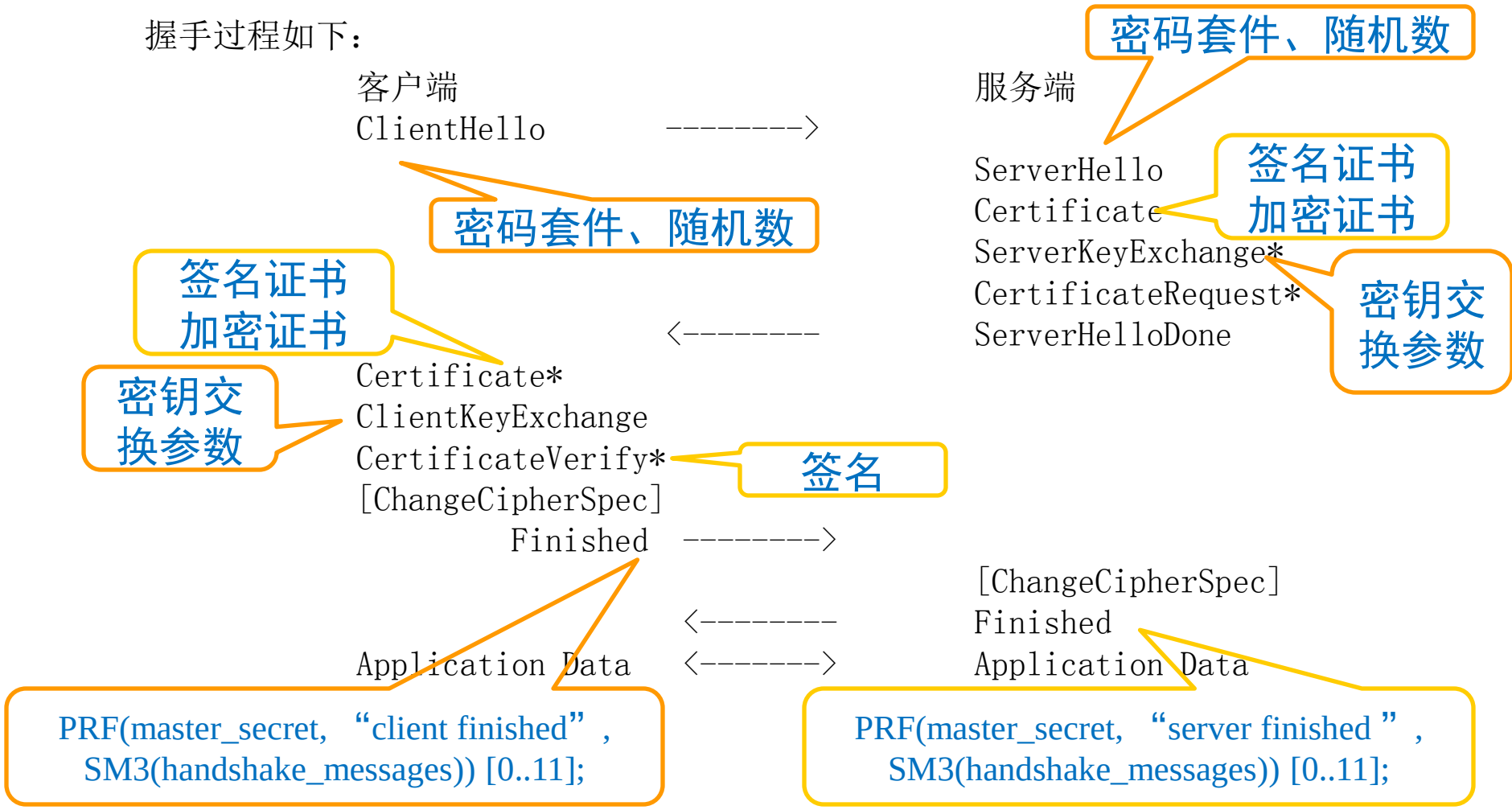


安全参数
客户端写校验密钥
服务端写校验密钥
客户端写密钥
服务端写密钥

标准的主要内容解读 握手协议

- 交换hello消息来协商密码套件，交换随机数，决定是否会话重用
- 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、握手过程的真实性和完整性

标准的主要内容解读 握手协议



标准的主要内容解读 握手协议

序号	密码套件	服务端证书消息	服务端密钥交换消息	客户端证书消息	客户端密钥交换消息
1	ECDHE_SM1_SM3	服务端的签名证书和加密证书	服务端密钥交换参数和签名数据	客户端的签名证书和加密证书	客户端密钥交换参数
2	ECC_SM1_SM3	服务端的签名证书和加密证书	签名数据	客户端的签名证书和加密证书	服务端加密公钥加密的预主密钥
3	IBSDH_SM1_SM3	服务端标识和IBC公共参数	IBSDH算法的服务端密钥交换参数和签名数据	客户端标识和IBC公共参数	客户端密钥交换参数
4	IBC_SM1_SM3	服务端标识和IBC公共参数	IBC算法的服务端密钥交换参数和签名数据	客户端标识和IBC公共参数	服务端加密公钥加密的预主密钥
5	RSA_SM1_SM3	服务端的签名证书和加密证书	签名数据	客户端的签名证书和加密证书	服务端加密公钥加密的预主密钥
6	RSA_SM1_SHA1	服务端的签名证书和加密证书	签名数据	客户端的签名证书和加密证书	服务端加密公钥加密的预主密钥

标准的主要内容解读 握手协议

序号	密码套件	服务端证书消息	服务端密钥交换消息	客户端证书消息	客户端密钥交换消息
7	ECDHE_SM4_SM3	服务端的签名证书和加密证书	服务端密钥交换参数和签名数据	客户端的签名证书和加密证书	客户端密钥交换参数
8	ECC_SM4_SM3	服务端的签名证书和加密证书	签名数据	客户端的签名证书和加密证书	服务端加密公钥加密的预主密钥
9	IBSDH_SM4_SM3	服务端标识和IBC公共参数	IBSDH算法的服务端密钥交换参数和签名数据	客户端标识和IBC公共参数	客户端密钥交换参数
10	IBC_SM4_SM3	服务端标识和IBC公共参数	IBC算法的服务端密钥交换参数和签名数据	客户端标识和IBC公共参数	服务端加密公钥加密的预主密钥
11	RSA_SM4_SM3	服务端的签名证书和加密证书	签名数据	客户端的签名证书和加密证书	服务端加密公钥加密的预主密钥
12	RSA_SM4_SHA1	服务端的签名证书和加密证书	签名数据	客户端的签名证书和加密证书	服务端加密公钥加密的预主密钥

标准的主要内容解读 网关到网关协议

- 控制报文
  - 网络层保护域
    - 子网与子网掩码
    - 网络地址范围
  - 传输层保护域
    - 传输层协议
    - 传输层端口
- 数据报文
  - 承载协议-记录层协议
  - 隧道状态-SSL连接状态

目录

- 标准的适用范围和作用
- 标准的编制思路和技术路线
- 标准的主要内容解读
- 标准应用时的注意事项
- 应用举例

标准应用时的注意事项（一）

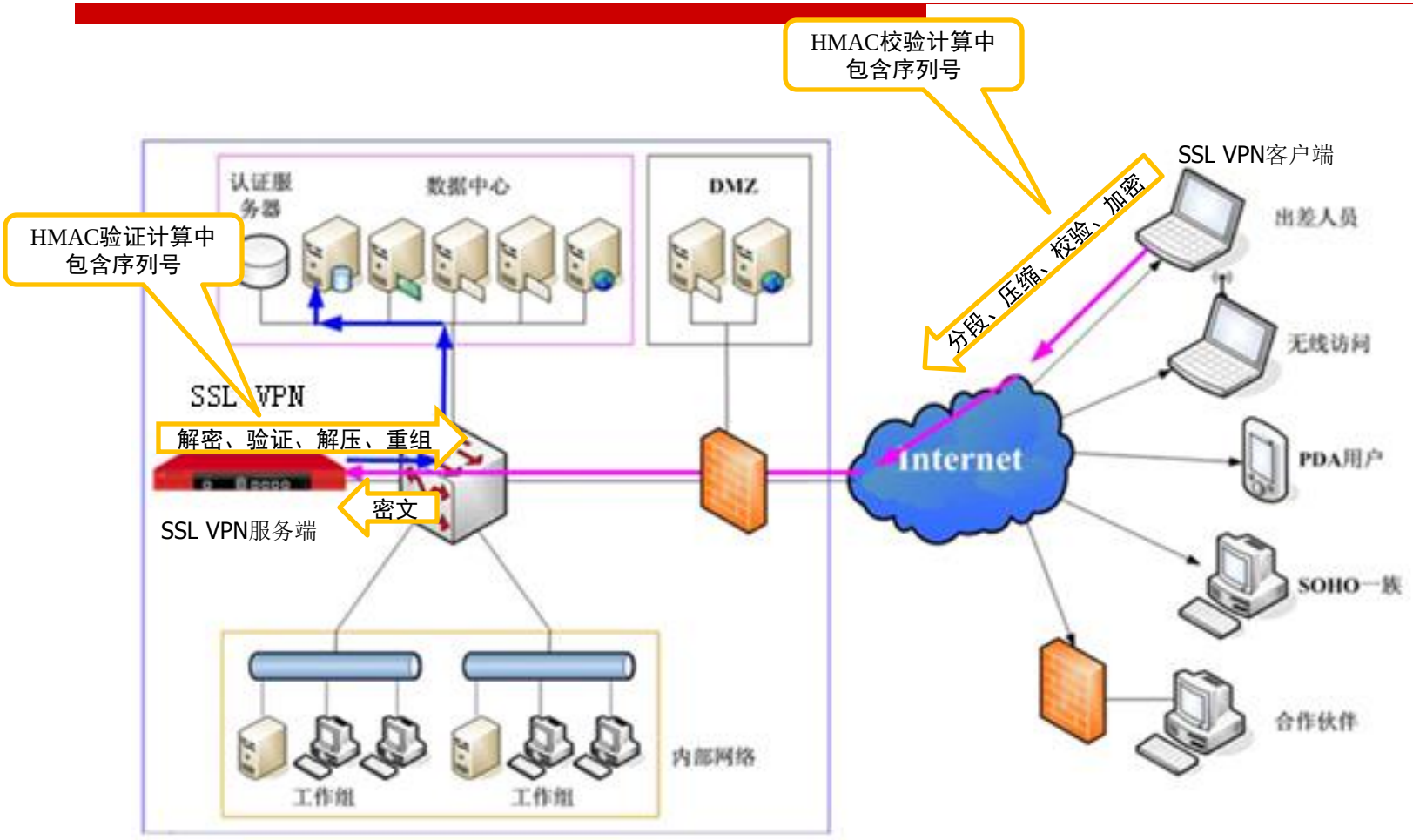
- 随机数生成算法生成的随机数应能通过《GM/T 0005随机性检测规范》规定的检测
- 当使用SM2算法进行加密、签名验证和密钥交换时，应符合《GM/T 0009 SM2密码算法使用规范》
- 加密密钥对要通过CA从密钥管理中心申请，私钥保护方法见《GM/T 0014 数字证书认证系统密码协议规范》
- SM2证书的结构及定义见《GM/T 0015基于SM2密码算法的数字证书格式规范》
- 实现ECC和ECDHE的算法为SM2；实现IBC和IBSDH的算法为SM9；RSA算法模长需2048以上

标准应用时的注意事项（二）

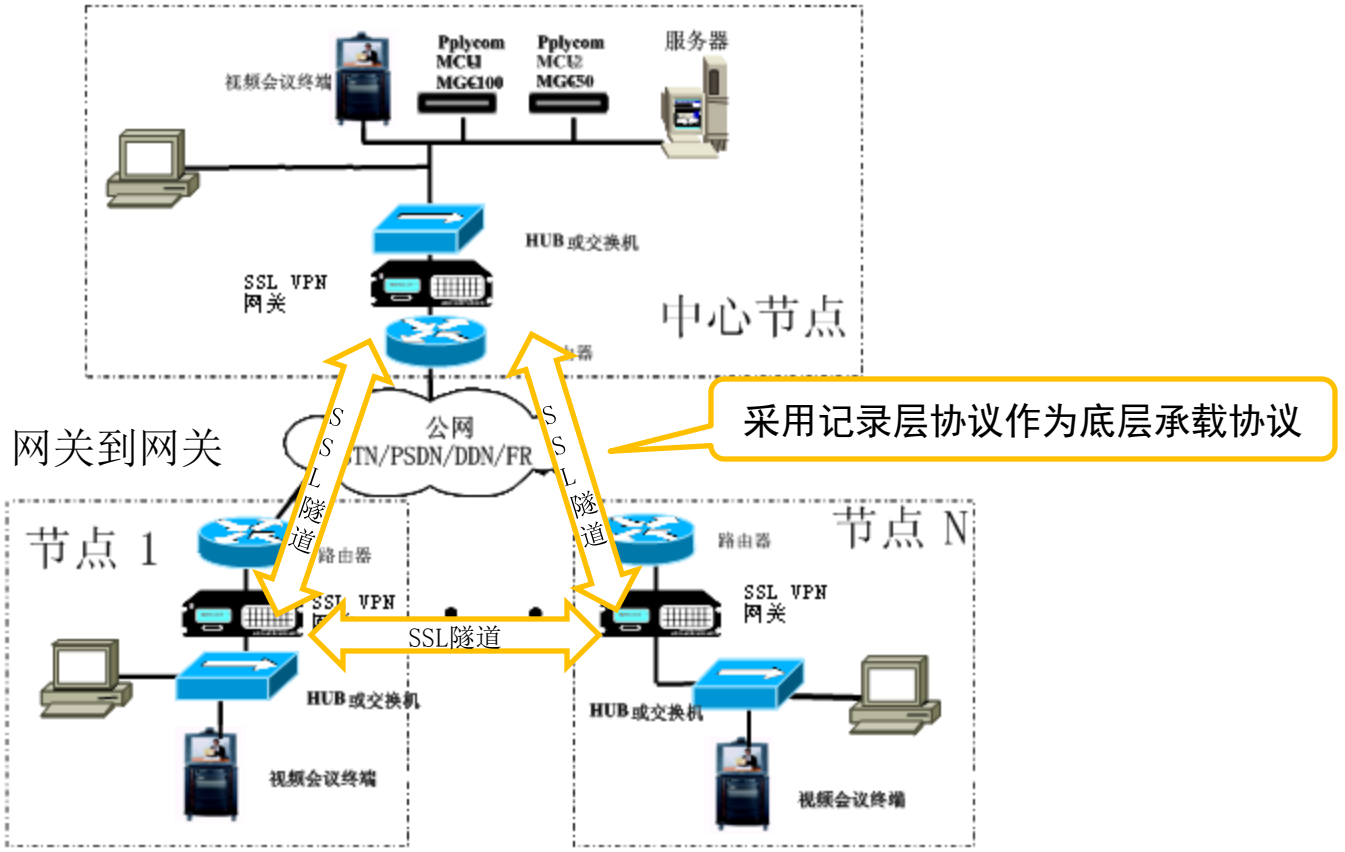
- 本规范不与TLS1.1/TLS1.2兼容
- 对称加密算法可采用SM1或SM4分组密码算法
- 非对称加密算法可采用SM2或RSA2048
- 密码杂凑算法可采用SM3或SHA1
- ECDHE密钥交换模式采用的是《GM/T 0009 SM2密码算法使用规范》中的SM2密钥交换方法，共享秘密的计算过程包括交换的参数、对方公钥和本地私钥

目录

标准的主要内容解读 应用举例



标准的主要内容解读 应用举例



NAT穿越、QoS保障上具有优势

感谢参与！