

中华人民共和国通信行业标准

YD/T 2909-2015

移动通信网络域安全认证框架

Mobile network domain security authentication framework

(3GPP TS 33.310 V9.5.0, Network Domain Security (NDS);
Authentication Framework (AF), IDT)

2015-07-14 发布

2015-10-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	III
引 言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义、缩略语和符号	3
3.1 术语和定义	3
3.2 缩略语和符号	3
4 公钥基础设施 (PKI) 介绍	4
4.1 手动交叉认证	4
4.2 桥CA的交叉认证	4
5 NDS/AF的架构与使用场景	5
5.1 NDS/AF的PKI架构	5
5.2 应用场景	7
6 配置	14
6.1 证书配置	14
6.1a CRL配置	17
6.2 IKE协商与配置	17
6.2a TLS配置	18
6.3 路径确认	18
7 架构与机制的详细描述	19
7.1 知识库	19
7.2 生命周期管理	21
7.3 交叉证书	21
7.4 废除SEG/TLS CA交叉证书	22
7.5 在NDS/IP端实体之间Za接口上使用IKE建立安全连接	22
7.5a 使用TLS建立安全连接	22
7.5b 在NDS/IP实体之间Zb接口上建立安全连接	22
7.6 CRL管理	22
8 对于NDS/IP 网元和安全网关的后向兼容性	23
9 基站的证书注册过程	23
9.1 概要	23
9.2 架构	23
9.3 安全机制	24

9.4 证书简介.....	24
9.5 CMPv2简介.....	26
9.6 CMPv2传输.....	29
附录A（规范性附录） 重要和非重要的证书扩展.....	30
附录B（资料性附录） 对简单信任模型的决定.....	31
附录C（资料性附录） SEGs的CRL库接入协议.....	36
附录D（资料性附录） 在CR中存储交叉证书的结论.....	37
附录E（资料性附录） TLS协议的规格.....	38
附录F（资料性附录） TLS证书手动处理.....	39
附录G（资料性附录） 初始登记的样本CMPv2信息流.....	40

前 言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准使用翻译法等同采用3GPP TS 33.310 V9.5.0 “网络域安全；认证框架”（Network Domain Security (NDS); Authentication Framework (AF)）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：华为技术有限公司、中国信息通信研究院、中国移动通信集团公司、中国联合网络通信集团有限公司、上海贝尔股份有限公司、诺基亚西门子通信（上海）有限公司。

本标准主要起草人：崔洋、黄迎新、胡志远、崔媛媛、齐旻鹏、张尼、陆伟。

引 言

在移动通信系统中，越来越多的网元设备和接口需要安全机制加以保护，其中，特别是对于可灵活扩展的实体认证框架(AF)有着日趋迫切的需求。本标准移动通信网提供了一种高度可扩展的身份认证框架。该框架遵循网络域安全研究的前后关系，有效地聚焦于核心网实体的控制面，因此 AF 可以为所有使用 NDS/IP 的网络节点提供有效安全的实体认证。此外，基于可信模型的可行性分析与效果预测，本标准还对 AF 实施所涉及的协议与证书特性也相应加以分析整理。依据上述分析得出安全认证框架的具体实施条件，以使电信运营商可以结合 IP 安全技术（IPsec）与公钥基础设施技术（PKI）来提供对网络域节点的有效保护。具体的，本标准描述了移动通信网的网络域安全认证框架，包括 PKI 交叉认证、CA 证书管理(包括申请、创建、吊销、更新)、网元实体证书管理、网元设备 CA 管理和基站的证书自动申请等。

移动通信网络域安全认证框架

1 范围

本标准适用于使用 NDS/IP 或者 TLS 的网元(NE)的认证。

对于 3GPP TS 33.210 中所述的 NDS/IP, 本标准包括在相应 Za 接口的安全网关 (SEG) 的认证和在 Zb 接口的网元之间以及网元和安全网关之间的认证。运营商域内的网络设备 (即网元和安全网关) 的认证是运营商内部的事情, 这与 3GPP TS 33.210 中规定一致, 即强制部署 Za 接口, 运营商自己决定是否配置 Zb 接口, 因为 Zb 接口为可选。如果是在相同运营商的两个安全域之间的 Za 接口或者 Zb 接口, 证书的有效性可能受限于运营商的域。

注: 假如两个安全网关是同一个管理中心 (例如, 由相同移动运营商拥有) 下两个不同网络域的相互连接, 那么还是需要部署 Za 接口, 但是 Za 接口的使用由运营商决定。

基于 IP 协议的 NDS 架构如图 1 所示:

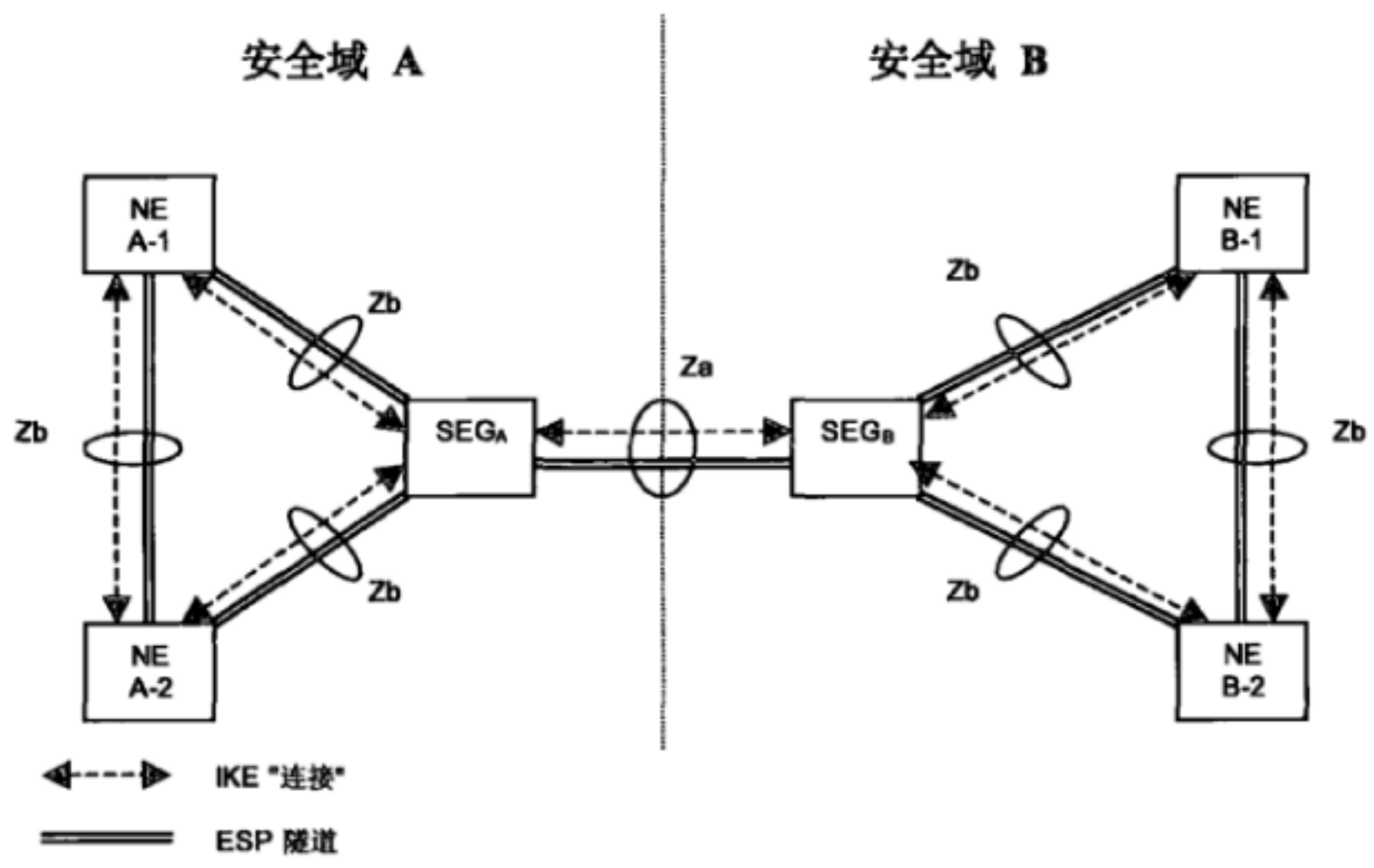


图 1 3GPP TS 33.210 中基于 IP 协议的 NDS 架构

对于 TLS, 本标准集中于运营商之间的链路的 TLS 实体的认证。例如, 对于 IMS 和非 IMS 网络 3GPP TS 33.203 和在 3GPP TS 33.220 里的 Zn'接口上的运营商间的通信, TLS 有详细说明。运营商内链路的 TLS 实体的认证视为运营商内部的事情。然而, 当所有的 TLS 网元和 PKI 基础设施属于同一个运营商时, NDS/AF 很容易适配到运营商内部的使用场景, 因为这只是运营商之间使用场景的简化。证书的有效性受限于运营商的域。一个附录包括关于 TLS 证书手动处理的信息, 以防基于 TLS 的 NDS/AF, 不能实现自动登记和撤销。

2 规范性引用文件

下列文件对于本文件的应用必不可少。凡是注日期的引用文件, 仅所注日期的版本适用于本文件。凡是不注日期的引用文件, 其最新版本 (包括所有的修改单) 适用于本文件。

3GPP TR 21.905 Vocabulary for 3GPP Specifications 3GPP 规范的词汇表

3GPP TS 33.203	Access security for IP-based services	基于 IP 业务的接入安全
3GPP TS 33.210	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security	网络域安全; IP 网络层安全
3GPP TS 33.220	Generic Authentication Architecture: Generic Bootstrapping Architecture	通用认证框架: 通用自举架构
IETF RFC 1035	Domain Names-Implementation and Specification	域名——实现和规范
IETF RFC 1981	Path MTU Discovery for IP version 6	IPv6 的路径 MTU 发现
IETF RFC 2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions	轻量级目录访问协议: 属性语法定义
IETF RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP	X.509 因特网公钥基础设施在线证书状态查询协议
IETF RFC 2817	Upgrading to TLS Within HTTP/1.1	HTTP/1.1 升级到 TLS
IETF RFC 2818	HTTP Over TLS	基于 TLS 的 HTTP
IETF RFC 2986	PKCS#10 Certification Request Syntax Specification Version 1.7	证书请求语法规范
IETF RFC 3749	Transport Layer Security Protocol Compression Methods	传输层安全协议的压缩方式
IETF RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol	互联网 X.509 公钥基础设施证书管理协议
IETF RFC 4211	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)	X.509 公钥基础设施证书请求消息格式
IETF RFC 4346	The Transport Layer Security (TLS) Protocol Version 1.1	传输层安全 TLS v1.1
IETF RFC 4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX	IKEv1/ISAKMP、IKEv2 和 PKIX 的互联网 IP 安全 PKI 配置
IETF RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2	传输层安全 TLS v1.2
IETF RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	X.509 因特网公钥基础设施证书及证书撤销列表
IETF RFC 5922	Domain Certificates in the Session Initiation Protocol (SIP)	会话初始化协议中的域证书
IETF RFC 5924	Extended Key Usage (EKU) for Session Initiation Protocol (SIP) X.509 Certificates	会话初始化协议中 X.509 证书的扩展的密钥使用

IETF RFC 6712	Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)	X.509 公钥基础设施—HTTP CMP 传输协议
PKI 基础	PKI basics – A Technical Perspective", November 2002, http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf	技术前景

3 术语、定义、缩略语和符号

3.1 术语和定义

3GPP TR 21.905 列出的及下列术语和定义适用于本文件。

3.1.1

互连认证中心 Interconnection CA

一个特殊运营商颁发交叉证书给与该运营商相互连接的其他域的 SEGs CAs。

3.1.2

互连协议 Interconnection Agreement

由两个运营商建立安全通信的协议。这是出于保护运营商之间不同形式通信的目的，例如：GPRS 漫游、MMS 相互连接、WLAN 漫游和 IMS 相互连接。

3.1.3

本地证书库 Local CR

存有交叉证书的证书库。

3.1.4

本地证书撤销列表 Local CRL:

包含交叉证书撤销列表的列表。

3.1.5

预共享密钥 Pre-Shared Key

NDS/IP 中 SEG 之间的 IKE 使用的认证方法。

3.1.6

公共证书撤销列表 Public CRL

包含 SEG 撤销列表和 CA 证书的列表，且能被其他运营商访问。

3.1.7

安全网关认证中心 SEG CA

在一个特殊运营商域内给 SEGs 颁发证书的认证中心。

3.2 缩略语和符号

下列缩略语和符号适用于本文件。

AF	Authentication Framework	认证框架
CA	Certification Authority	认证中心
CR	Certificate Repository	证书库
CRL	Certificate Revocation List	证书撤销列表

GBA	Generic Bootstrapping Architecture	通用自举架构
IMS	IP Multimedia Subsystem IP	多媒体子系统
NDS	Network Domain Security	网络域安全
PKI	Public Key Infrastructure	公钥基础设施
POP	Proof Of Possession	证明所有权
PSK	Pre-Shared Key	预共享密钥
RA	Registration Authority	注册中心
SEG	Security Gateway	安全网关
VPN	Virtual Private Network	虚拟专用网络
Za	Interface between SEGs belonging to different networks/security domains (a Za interface may be an intra or an inter operator interface)	不同网络或安全域之间的安全网关的接口（该接口可能在同一个运营商内部，也可能在不同运营商之间
Zb	Interface between SEGs and NEs and interface between NEs within the same network/security domain	同一网络或同一安全域之间的安全网关的接口和网元及网元之间的接口

4 公钥基础设施（PKI）介绍

PKI 论坛的“PKI 基础——技术前景”对 PKI 技术进行了简单中立的介绍。因此，在介绍部分只描述了交叉认证的两个方面。

交叉认证是在两个认证中心之间建立信任关系的一个过程。在认证中心 B 交叉认证认证中心 A 时，认证中心 A 已经选择由认证中心 B 颁发的可信的证书。交叉认证过程使处于两个认证中心下的用户信任由对方认证中心颁发的证书。在本标准中，信任等同于能够认证。

4.1 手动交叉认证

相互的交叉认证直接建立在两个认证中心之间。这个方法常称之为手动交叉认证。在手动交叉认证中，认证中心在本地决定信任。当认证中心 A 选择信任认证中心 B 时，认证中心 A 签署认证中心 B 的证书，并且在本地分发这个新证书（由 A 签名的 B 的证书）

这种方法的缺点是，它常常会导致出现这样的场景：做出信任决定的实体需要获得很多证书/对于每一个本地认证中心愿意信任的安全域，需要有一个由本地认证中心签名的证书。然而，所有的证书都能在本地图配置，且在本地签名，因此，证书管理非常灵活。

4.2 桥 CA 的交叉认证

桥 CA 能减少为用于证书校验的实体所配置的证书数量。当两个认证中心通过桥 CA 做相互交叉认证时，该两个认证中心不必知道彼此，能信任彼此，因为在这种模型中，信任是具有传递性的（A 信任桥 CA，桥 CA 信任 B，因此 A 信任 B，反之亦然）。桥 CA 在认证中心之间表现得就像一个桥。但是，两个认证中心应信任桥 CA 会做正确的事情。所有关于信任的决定都能委派给桥 CA，桥 CA 在一些使用场合是再好不过的。如果桥 CA 决定交叉认证一个认证中心 M，以前交叉认证过的认证中心自动开始信任 M。

在所有实体共享一个公共的认证中心场景中，桥 CA 形式的交叉非常实用。如果一个认证中心需要对来自桥 CA 的信任或接入控制进行限制，那么该认证中心还需额外执行这些限制条件。

5 NDS/AF 的架构与使用场景

认证中心类型的定义如下：

- 安全网关的认证中心 (SEG CA)：一个 CA 给指定运营商域内的安全网关颁发证书。
- 网络实体的认证中心 (NE CA)：一个 CA 给指定运营商域内的网络实体颁发 IPsec 证书，而且这些证书只限定使用于 Zb 接口 (Zb：网络域内的实体之间或网络域实体与安全网关之间的接口)。
- TLS 客户端认证中心 (TLS client CA)：一个 CA 给指定运营商域内的 TLS 实体颁发 TLS 客户端证书。
- TLS 服务器认证中心 (TLS server CA)：一个 CA 给指定运营商域内的 TLS 实体颁发 TLS 服务器证书。
- 互连认证中心 (Interconnection CA)：一个 CA 代表一个指定运营商将交叉证书颁发给其它域内的 SEG CA、TLS 客户端 CA 以及 TLS 服务器 CA，使用这些交叉证书能实现运营商的 SEGs、TLS 实体的互连。

互连 CA 的公钥安全地存储在运营商域内的各个 SEG 和 TLS 实体中，这就能够使 SEG 和 TLS 实体相互验证交叉证书。假设每个运营商域内包含几十个而不是几百个 SEG 或 TLS 实体。

运营商可以将两个或两个以上的如上所述的 CA 合并。比如，同一个 CA 可以用来颁发实体 TLS 证书以及 IPsec 证书。另外，同一个 CA 也可以用来颁发实体证书和交叉证书。

NDS/AF 最初是基于一个简单的信任模型 (参见附录 B)，该模型避免引入传递性信任或/和额外认证信息。该简单模型隐含手动的交叉认证。

5.1 NDS/AF 的 PKI 架构

本条定义了 NDS/AF 的 PKI 架构。目标是定义一个灵活且简单的架构，并能做到与其它实现方式进行互操作。

如下描述的架构使用了简单接入控制方法，即每一个经过认证的实体都将得到服务。可能会实现更加精细的接入控制，但这不属于本标准的研究范围。

本架构不依赖于桥 CA，而是在不同安全域之间直接使用交叉证书，这使 SEG 和 TLS 实体中的策略配置变得更加简便。

5.1.1 总体架构

除非运营商选择合并多个 CA，否则每个安全域至少要有有一个 SEG CA，NE CA，TLS 客户端 CA 或 TLS 服务器 CA，以及一个专属于运营商的互连 CA。

一个域中的 SEG CA 将证书颁发给该域内的 SEGs，这些 SEGs 与其它域内的 SEGs 存在相互连接，即 Za 接口。SEG 证书也可以用在 Zb 接口上与 NE 进行相互通信。NE CA 将证书颁发给 NEs，用来实现 NE 之间的通信以及 NE 与可信任域内的 SEGs 之间的通信，即 Zb 接口。TLS 客户端 CA 将证书颁发给该域内需要与其它域内的 TLS 服务器建立 TLS 连接的 TLS 用户。TLS 服务器 CA 将证书颁发给域内需要与其它域内的 TLS 用户建立 TLS 连接的 TLS 服务器。互连 CA 将证书颁发给 SEG CAs、TLS 客户端 CAs 或与本域内的 SEG、TLS 客户端存在相互连接的其它域内 TLS 服务器 CAs。本标准描述了需要的各种证书的总配置 (profile)，同时也描述了一种生成交叉证书的方法。

总体而言，所有的证书都应基于 IETF RFC 5280。

5.1.1.1 NDS/IP 场景

以下描述了使用 SEG CAs 颁发 IPsec 证书的架构。

SEG CA 应该将证书颁发给使用 Za 接口的安全网关。当安全域 A 中的 SEG 与安全域 B 中的 SEG 建立安全连接时，它们应当能相互认证。相互认证是由 SEG CAs 颁发给 SEGs 的证书来实现的。当各个域间建立互连时，互连 CA 就交叉认证了对等运营商的 SEG CA。生成的交叉证书需要本地配置于每个域中。对于安全域 A 中的与安全域 B 间存在 Za 接口的 SEG 来说，由安全域 A 的互连 CA 为安全域 B 的 SEG CA 生成的交叉证书应该有效且可用。同样的，对于安全域 B 中的与安全域 A 间存在 Za 接口的 SEG 来说，由安全域 B 的互连 CA 为安全域 A 的 SEG CA 生成的交叉证书应该有效且可用。

基于 IPsec 证书来认证 SEGs 和 NEs 的总体架构如图 2 所示。

注：为了避免重复，一个潜在的 CA 在图 2 中并没有表现出来。

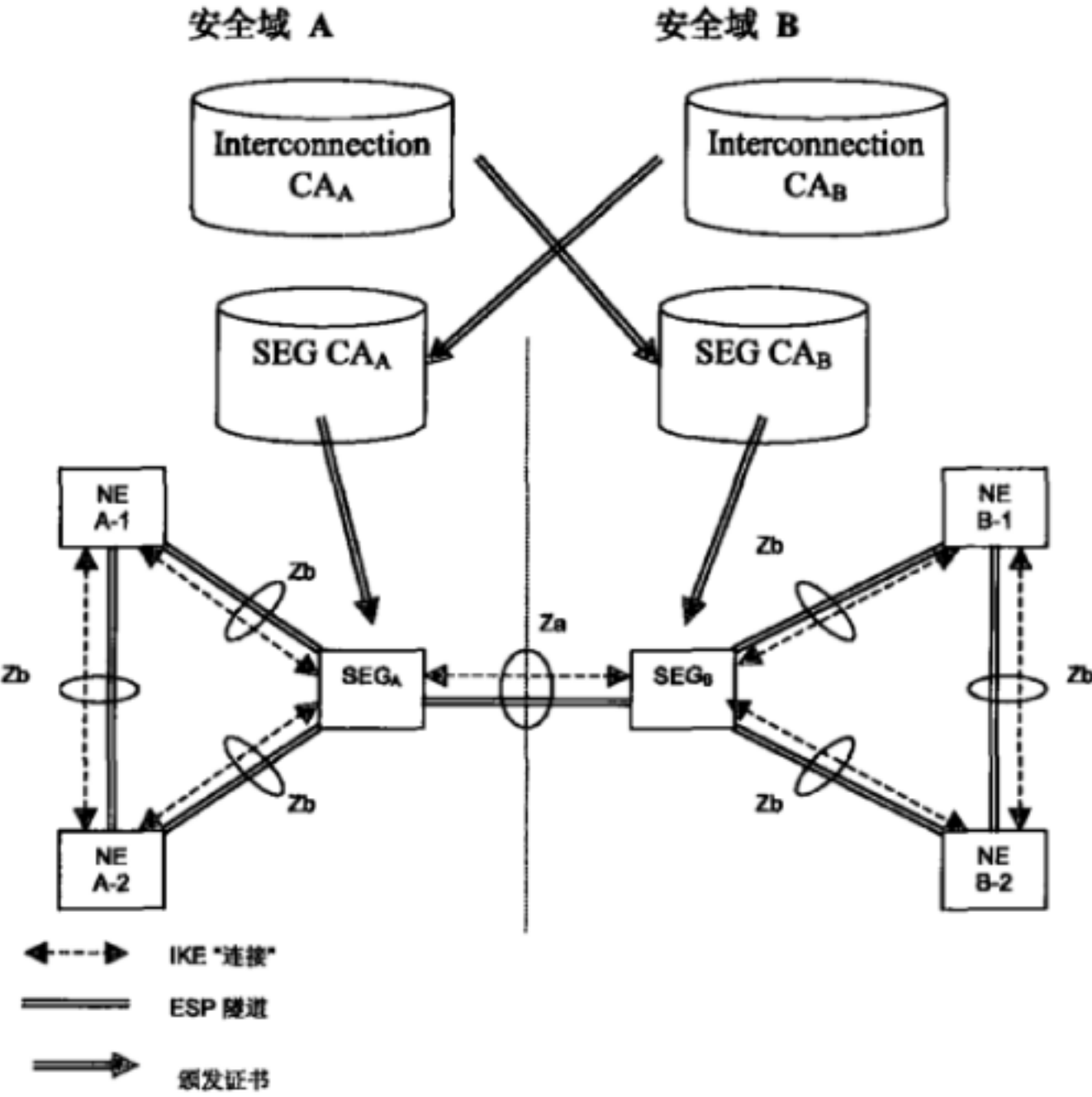


图 2 NDS/IP 场景下信任校验路径

交叉认证之后，SEG_A 就能确认路径：SEG_B -> SEG CA_B -> 互连 CA_A。安全域 A 内的所有实体只信任安全域 A 内的互连 CA_A 颁发的证书。

同样地，SEG_B 能确认路径：SEG_A -> SEG CA_A -> 互连 CA_B。该路径在安全域 B 内可确认，因为路径终止于一个可信任的证书（安全域 B 的互连 CA_B）。

互连 CA 路径中的第二张证书进行签名。例如，在安全域 A 中，SEG CA_B 的证书是由安全域 A 中的互连 CA 在执行交叉认证时进行签名。

5.1.1.2 TLS 场景

以下描述了使用 TLS CAs 颁发 TLS 证书的架构。

TLS 客户端 CA 应该将证书颁发给其安全域内的 TLS 用户。同样地，TLS 服务器 CA 应将证书颁发给其域内的 TLS 服务器。当安全域 A 中的 TLS 实体与安全域 B 中的 TLS 实体建立安全连接时，它们应当能相互认证。互认证是由 TLS 客户端/服务器 CAs 颁发给 TLS 实体的证书来实现。当各个域间建立互连时，互连 CA 就交叉认证了对等运营商的 TLS 客户端/服务器 CAs。生成的交叉证书只需要本地配置于每个域中。对于安全域 A 中需要与安全域 B 连接的 TLS 实体来说，由安全域 A 的互连 CA 为安全域 B

的 TLS 客户端/服务器 CA 生成的交叉证书应该有效且可用。同样的，对于安全域 B 中需要与安全域 A 连接的 TLS 实体来说，由安全域 B 的互连 CA 为安全域 A 的 TLS 客户端/服务器 CAs 生成的交叉证书应该有效且可用。

TLS 实体认证的总体架构如图 2a 所示。

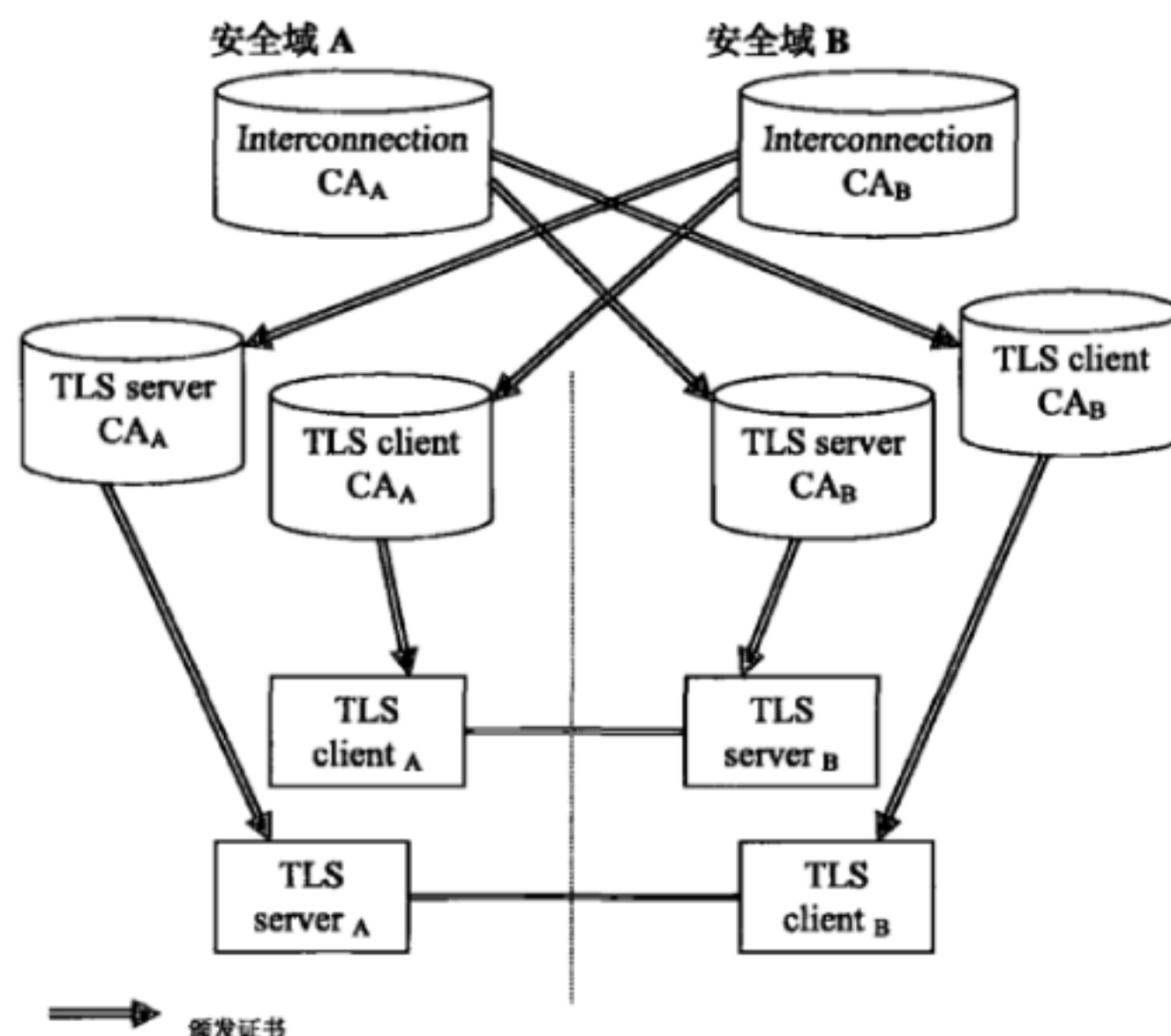


图 2a TLS 场景下信任校验路径

交叉认证之后，TLS client A 就能确认路径：TLS server B -> TLS server CA_B -> 互连 CA_A。安全域 A 内的所有实体只信任安全域 A 内互连 CA_A 所颁发的证书。

同样地，TLS client B 应能确认路径：TLS server A -> TLS server CA_A -> 互连 CA_B。该路径在安全域 B 内验证，因为路径终止于一个可信任的证书（由安全域 B 内互连 CA_B 颁发）。

互连 CA 对路径中的第二张证书进行签名。例如，在安全域 A 中，TLS 服务器 CA_B 及 TLS 客户端 CA_B 的证书是由安全域 A 中的互连 CA 在执行交叉认证时进行签名。

5.2 应用场景

5.2.1 运营商注册：互连协议的生成

当运营商进行互连协定时，两个不同安全域中的 SEGs 或 TLS 实体需要建立一个安全连接。在两个安全域间创建互连协定的第一步是使用两个安全域中的互连 CA 来创建交叉证书。

运营商之间的交叉认证可以使用各种不同的协议，但认证中心应该支持 IETF RFC 2986 中所述的 PKCS#10 来做证书请求。SEG CA、TLS 客户端 CA 及 TLS 服务器 CA 生成一个 PKCS#10 证书请求，然后将其发送给其它运营商的互连 CA。不规定传输 PKCS#10 证书请求的方式，但需要保证传输的安全。PKCS#10 可以通过软盘或者签名过的电子邮件进行传输。PKCS#10 请求包括认证中心的公钥，以及请求交叉证书的认证中心的名称。当互连 CA 接受了该请求后，将为发起请求的 CA 生成一个新的交叉证书。同时，互连 CA 应使其域内会用到该交叉证书的 SEGs 和 TLS 实体对该交叉证书可用。另一域中获得的 SEG CA 的交叉证书存储在本地证书库中，所有需要接入到其它安全域中的 SEGs 应当使用 IETF RFC 2252 中所述的该本地证书库。TLS 客户端 CAs 与 TLS 服务器 CAs 的交叉证书对 TLS 实体可用，通过将证书存储在 TLS 实体的可信 CA 中，或者将交叉证书存储在本地证书库中，所有需要接入到其它

安全域中的 TLS 实体应当使用 IETF RFC 2252 中所述的 LDAP 协议来访问该本地证书库。

交叉认证是手动性的操作，因此 PKCS#10 是一个实现互连协定的好方法。

互连协定的创建只使用互连 CA 的私钥。运营商没有必要使用各自的 SEG CA, TLS 客户端 CA 或 TLS 服务器 CA 的私钥来创建互连协定。

当生成新的交叉证书时，互连 CA 应该使用基本的限制扩展（见 IETF RFC 4210 中 4.2.1.10），并将路径长度设置为零。这样可防止新的交叉证书用来签名新的 CA 证书。证书的有效性的时间应该足够长久。一旦交叉证书有效性到期，需要重新做一次交叉认证。

当新的交叉证书可用于 SEG 时，SEG 中需要配置对等 SEG 网关的 DNS 名称或 IP 地址，其相互认证基于新生成的交叉证书。

当新的交叉证书可用于 TLS 实体时，TLS 实体就可以认证对等网络里的 TLS 实体。认证基于新生成的交叉证书。

两个对等运营商的证书层次如图 3 所示。

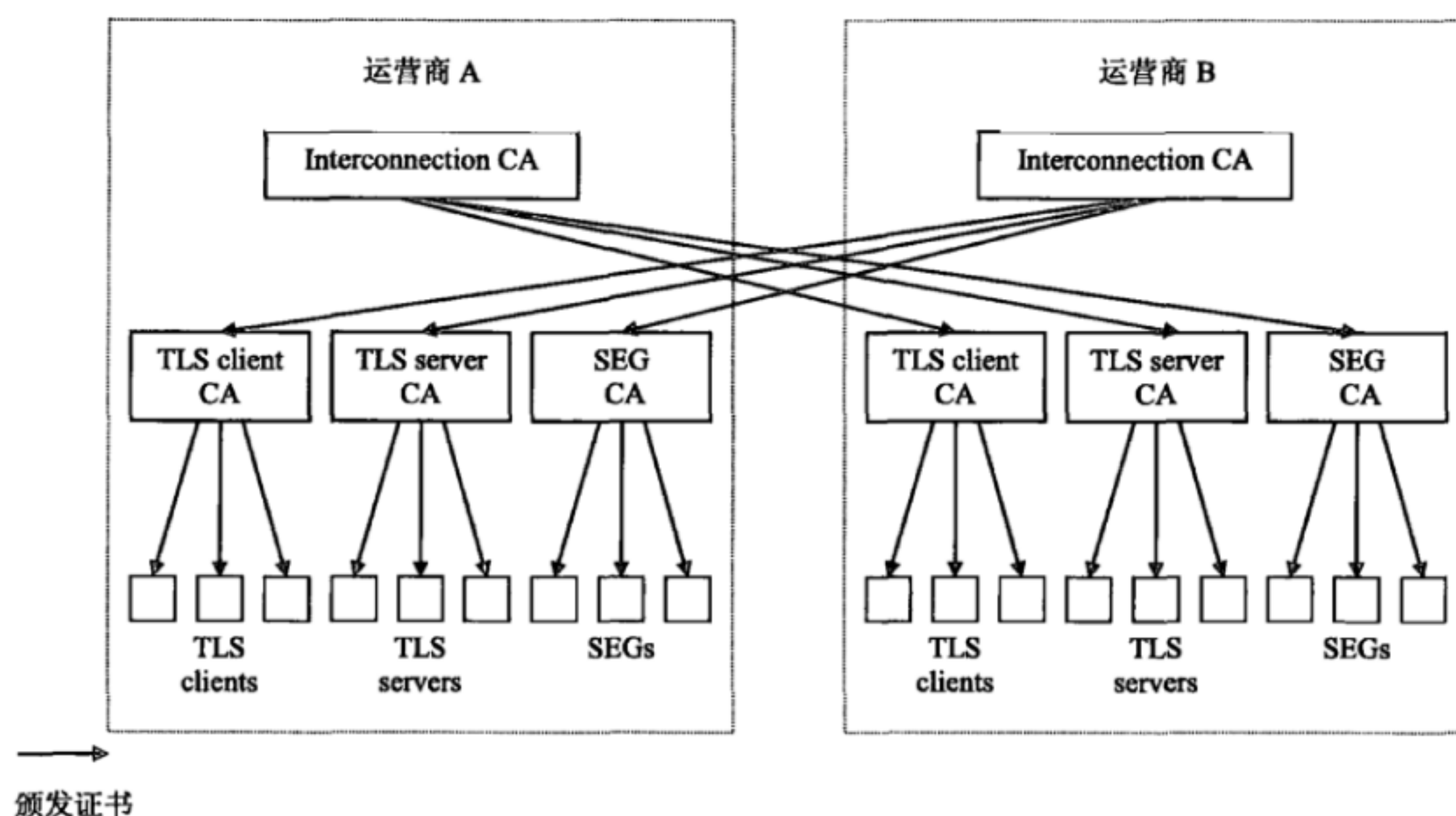


图 3 证书层次

5.2.2 安全通信的建立

5.2.2.1 NDS/IP 场景

5.2.2.1.1 NDS/IP 场景下的 Za 接口

建立互连协定并且完成要求的预备证书管理操作之后，运营商开始为建立 SEG-SEG 连接而配置其域内 SEG，依据 NDS/IP 规范 3GPP TS 33.210 来建立 SA。

在每个连接配置中，远端的 SEG DNS 名称或者 IP 地址需指定。只有本地互连 CA 及 SEG CA 配置为可信的 CAs。只要运营商的 SEG CA 已被交叉认证，就可以使用虚拟私有网（VPN）连接配置来实现相应接入。

下面是从运营商 A 的 SEG（发起者）角度出发的连接协商流程。运营商 B 的 SEG（回应者）应该进行相似的操作。

——连接初始化时，运营商 A 的 SEG A 将其 SEG 证书及对应的数字签名包含在 IKE Main Mode

message 3 中（对于 IKEv1），或者包含在 IKE_AUTH exchange 中（对于 IKEv2）；

——SEG A 接收远端 SEG B 的证书和签名；

——SEG A 验证远端 SEG B 的签名；

——通过对运营商 B 的 CRL 数据库的 CRL 检查，SEG A 验证 SEG B 证书的有效性。假如 SEG 不能成功完成 CRL 验证，应做错误处理并中断安全通道的建立；

——SEG A 通过执行以下步骤来验证 SEG B 的证书；

- SEG A 从运营商 A 的证书库或本地缓存中获取运营商 B 的 SEG CA 的交叉证书；

- 通过对运营商 A 互连 CA 的 CRL 数据库的 CRL 检查，SEG A 验证运营商 B 的 SEG CA 的交叉证书的有效性。假如 SEG 不能成功完成 CRL 验证，应做错误处理并中断安全通道的建立；

- SEG A 使用运营商 A 的互连 CA 证书来验证运营商 B 的 SEG CA 交叉证书。如果运营商 A 的互连 CA 不是顶级 CA，还应认证互连 CA 的证书，否则可以认为互连 CA 的公钥是可信的。

如果启用的是 IKEv1，此时 IKE Phase 1 SA 已建立，然后应按照 NDS/IP 规范 3GPP TS 33.210 中描述的那样，并使用 PSK 认证机制来进行 Phase-2 SA 协商。

如果启用的是 IKEv2，此时 IKE_AUTH exchange 过程已完成。现在就可以按照 NDS/IP 规范 3GPP TS 33.210 中描述的那样，使用 PSK 认证方式来发起 IKEv2 CREATE_CHILD_SA exchange 过程。

注：对于互连通信（运营商—运营商），本标准为 SEG 提供了端到端的认证模式。假如使用 NDS/AF（IKE）认证来接入传输网（如 GRX）以及运用到端到端互连通信中，那么就需要使用多重安全通道或者点对点安全的 IPsec 机制及策略。但是，本标准的认证架构是独立于下层 IP 传输网的。

5.2.2.1.2 NDS/IP 场景下的 Zb 接口

该场景下，没有必要做交叉认证。两个网络设备属于同一运营商的管理域中，这样就由同一个顶层 CA 来检查认证授权。

下面是从 NE-A（发起者）角度出发的连接协商流程。同一域中的 NE-B 或 SEG-B（作为回应者）应该进行相似的操作。

——连接初始化时，运营商 A 的 NE-A 将其 NE 证书及相应的数字签名包含在 IKEv1 Main Mode message 3 中（对于 IKEv1 协议），或者包含在 IKE_AUTH exchange（对于 IKEv2 协议）。

——NE A 接收 NE B（或 SEG B）的证书和签名。

——NE A 验证 NE B（或 SEG B）的签名。

——通过该运营商的 CRL 数据库的 CRL 检查，NE A 验证 NE B（或 SEG B）证书的有效性。假如 NE 不能成功完成 CRL 验证，应做错误处理并中断安全通道的建立；

- 如果启用的是 IKEv1，此时 IKE Phase 1 SA 已建立，然后应按照 NDS/IP 规范 3GPP TS 33.210 中描述的那样，并使用 PSK 认证机制来进行 Phase-2 SA 的协商；

- 如果启用的是 IKEv2，此时 IKE_AUTH exchange 过程已完成。现在就可以按照 NDS/IP 规范 3GPP TS 33.210 中描述的那样，使用 PSK 认证方式来发起 IKEv2 CREATE_CHILD_SA exchange 过程。

5.2.2.2 TLS 场景

建立互连协定并且完成要求的预备证书管理操作之后，运营商开始为建立安全互连而配置其域内 TLS 实体。建立 TLS 互连的具体过程依赖于应用协议，不属于本标准范围。但是，总体流程将在本条余下部分中介绍。

通过将本地互连 CA 及 TLS client/server CA 存储在 TLS 实体的可信 CA 文件中, 可以将互连 CA 及 TLS client/server CA 配置为 TLS 实体可信任的 CA。远端运营商 TLS client/server CA 中的交叉证书也应该对 TLS 实体可用, 可将交叉证书存储到 TLS 实体的可信 CAs 列表中, 或者将交叉证书存储到本地证书库中, 所有需要与其它域通信的 TLS 实体应能接入到本地证书库 (比如使用 LDAP 协议)。只要某运营商的 TLS client CA 或 TLS server CA 被另一运营商交叉认证过, 就可与该另一运营商建立 TLS 安全连接。

下面是从运营商 A 作为 TLS client (TLSa) 与运营商 B 作为 TLS server (TLSb) 的角度出发的连接建立流程。TLS client 在运营商 B 中、TLS server 在运营商 A 中的场景应进行类似处理。以下流程基于 IETF RFC 5246 中的 TLS 握手协议。

——连接初始化过程中, TLSa 发送 ClientHello 消息给 TLSb。TLSb 首先回复一个 ServerHello 消息给 TLSa, 然后发送 ServerCertificate message, ServerKeyExchange message, 可选的 CertificateRequest message, 以及 ServerHelloDone message。ServerCertificate message 包含由运营商 B 的 TLS server CA 颁发的 TLSb 证书。当 TLSb 需要认证 TLSa 时, 才发送 CertificateRequest message。

——TLSa 接收来自 TLSb 的消息。

——TLSa 使用 TLSb 的公钥验证 ServerKeyExchange message。

——通过检查运营商 B 的 CRL 数据库的 CRL, TLSa 验证 TLSb 的证书有效性。假如对等的 TLS 实体不能成功通过 CRL 验证, 应做错误处理并中断安全通道的建立。

——TLSa 使用运营商 B 的 TLS server CA 的交叉证书来验证 TLSb 的证书, 流程如下:

——TLSa 从运营商 A 的证书库获取运营商 B 的 TLS server CA 的交叉证书, 或从 TLSa 证书库的本地缓存获取, 或在 TLSa 没有独立证书库的情况下, 从 TLSa 的本地证书存储获取。

- 通过检查运营商 A 的互连 CA 的 CRL 数据库的 CRL, TLSa 验证运营商 B 的 TLS server CA 的交叉证书的有效性。假如对等的 TLS 实体不能成功通过 CRL 验证, 应做错误处理并中断安全通道的建立;

- 如果互连 CA 不是顶级 CA, 那么 TLSa 需要使用运营商 A 的互连 CA 的证书来验证运营商 B 的 TLS server CA 的交叉证书, 否则可认为互连 CA 的公钥是可信的;

- 假如 TLSb 通过 CertificateRequest message 请求证书, 那么 TLSa 需要回复 Certificate message, 然后继续发送 ClientKeyExchange message, CertificateVerify message, 及 Finished message。只有 server 请求证书时才需发送 Certificate message。Certificate message 包括运营商 A 的 TLS client CA 颁发的 TLSa 证书。只有当 TLSa 的证书拥有签名能力时, 才会发送 CertificateVerify message, 为 client 证书提供单独认证;

- TLSb 接收 TLSa 的消息;

- TLSb 使用 TLSa 的公钥验证 ClientKeyExchange 及可选地验证 CertificateVerify message;

- 通过检查运营商 A 的 CRL 数据库的 CRL, TLSb 验证 TLSa 证书的有效性。假如对等的 TLS 实体不能成功通过 CRL 验证, 应做错误处理并中断安全通道的建立。

——TLSb 使用运营商 A 的 TLS client CA 的交叉证书来验证 TLSa 的证书, 执行如下步骤:

- TLSb 从运营商 B 的证书库获取运营商 A 的 TLS client CA 交叉证书、或从 TLSb 证书库的本地缓存获取、或在不使用单独的证书库的场景下从 TLSb 的本地证书存储中获取;

- 通过检查运营商 B 的互连 CA 的 CRL 数据库的 CRL, TLSb 验证运营商 A 的 TLS client CA 的交叉证书的有效性。假如对等的 TLS 实体不能成功通过 CRL 验证, 应做错误处理并中断安全通道的建立;

- 如果互连 CA 不是顶级 CA，那么 TLSb 需要使用运营商 B 的互连 CA 的证书来验证运营商 A 的 TLS server CA 的交叉证书，否则可认为互连 CA 的公钥是可信的。

- TLSb 发送 Finished message 来完成整个握手过程。

- TLSa 接收 Finished message 来完成整个握手过程。

如果握手过程能成功完成，就可以在 TLS 连接通道上进行安全的通信。

5.2.3 运营商注销：终止互连协定

当一个互连协定终止或者需紧急终止业务，所有相关的对等 SEG 应当使用具体的设备管理方法来删除 IPsec SA，同样所有相关的 TLS 实体应当终止任何与对等网络连通正进行的 TLS session，并禁止恢复这些 sessions（禁止 TLS session resumption 过程）。

每一个相关的运营商还应当将终止的运营商的互连 CA, SEG CA, TLS client CA 和 TLS server CA 的交叉证书列入其自己的本地 CRL 中。

5.2.3a 互连 CA 的注册

原则上说，运营商网络里只能存在一个互连 CA。但是使用两个以上的互连 CA 是可能的（这种情况下，运营商的所有互连 CA 的公钥应当安装在运营商的 SEG 或 TLS 实体中）。在互连 CA 注册过程中的操作见 5.2.1 的交叉证书部分的描述。如果互连 CA 功能从一个可信的组织机构移到另一个机构（比如，外购 CA 服务），那就可能存在上述情况。

5.2.3b 互连 CA 的注销

如果互连 CA 从网络移除，应保证所有由互连 CA 颁发给 SEG CA 或 TLS CA 的并且没有过期的证书，都应该列入 CRLs。

5.2.3c 互连 CA 认证的创建

互连 CA 证书可能不是运营商的顶级 CA，这意味着互连 CA 不是自签名的。如果互连 CA 证书是自签名的，那么该证书需要安全传输到每一个 SEG 或 TLS 实体并存储在其安全的存储器中，否则该证书应当用处理 SEG 或 TLS 实体证书一样的方法进行操作管理。

为了避免互连 CA 证书更新时需要做的交叉认证，互连 CA 证书的有效期限应当长于 SEG CA 或 TLS CA 证书的有效期限。

注：创建互连 CA 证书与其它运营商没有关系。

5.2.3d 互连 CA 证书的注销

假如互连 CA 的密钥对不再安全，那攻击者就可以使用该密钥对为自己颁发 SEG CA 或 TLS CA 证书，然后又可使用 SEG CA 或 TLS CA 证书来颁发 SEG 或 TLS 实体证书。因为可信的互连 CA 证书本地存储于 SEG 或 TLS 实体设备中或专用数据库中（即：在 IKE 及 TLS 握手过程中接收到的互连 CA 证书不应当被信任），因此攻击者需要攻破 SEG、TLS 实体或本地数据库才能建立一个安全连接。

不需要拆毁现已存在的安全连接。通过将旧的交叉证书以及任何由互连 CA 颁发的证书列入互连 CA 的 CRL（如果运营商还有签名该 CRL 的密钥）并且将它们从本地证书库中删除，这些证书就不能再用于正常业务。如果互连 CA 证书是自签名的，那么该证书就应当从运营商的 SEG 与 TLS 实体删除。如果互连 CA 证书由上级运营商 CA 颁发，那么互连 CA 证书应当由该上级 CA 撤销。

运营商需要生成一个新的互连 CA 密钥对，通过执行 5.2.3c 中的规定来创建互连 CA 认证，通过执行 5.2.1 中的规定来为与其互连的其它网络的 SEG CAs 或 TLS CAs 生成新的交叉证书。

注：撤销互连 CA 证书与其它运营商没有关系。

5.2.3e 互连 CA 证书的更新

在旧的互连 CA 证书到期前，需要更新互连 CA 证书。互连 CA 证书的更新包括重复 5.2.3 所叙述的步骤。更新过程应在旧的证书过期前完成。

注：更新互连 CA 证书与其它运营商没有关系。

5.2.4 SEG/TLS CA 注册

原则上运营商网络里只能分别有一个 SEG CA、TLS CA 及 TLS server CA，但是有两个以上的上述 CA 也是可能的。在 SEG/TLS CA 注册过程中的操作见 5.2.1 的交叉证书部分的描述。如果 CA 功能从一个可信任的机构转移到另一个（如，外购 CA 服务），那就可能存在上述每一类 CA 有多个的情况。

5.2.5 SEG/TLS CA 的注销

假如 SEG CA 或者 TLS CA 被从网络中删除，应保证将所有没有过期的 SEG CA 或 TLS CA 的证书以及由它们颁发给 SEGs 及 TLS 实体的证书列入 CRLs。同时，宜将颁发给 SEG CA 及 TLS CA 的没有过期的交叉证书列入 CRLs。

5.2.6 SEG/TLS CA 证书的创建

SEG/TLS CA 证书的创建过程中的操作见 5.2.1 的交叉证书部分的描述。

SEG CA 或 TLS CA 的证书不必要一定是运营商的顶级 CA，这意味着 SEG CA 或 TLS CA 的证书不是自签名的。一个选择是用运营商自己的互连 CA 来签名 SEG CA 或 TLS CA 的证书，因为互连 CA 是运营商 SEG 或 TLS 实体里已建立的可信点。假如 SEG CA 或 TLS CA 证书是自签名的，这些证书需要安全地传递到 SEG 或 TLS 实体并存储在安全的存储器中。

5.2.7 SEG/TLS CA 证书撤销

这是一个严重的威胁，因为要求撤销所有的由其它运营商的互连 CA 颁发给该 SEG CA 或 TLS CA 的交叉证书。

不需要拆毁现已存在的安全连接，除非它们近期才建立，也就是：在运营商发现 CA 密钥被攻破之后，但是在用来建立通道的交叉证书被撤销之前。

应保证将所有没有过期的 SEG CA 或 TLS CA 的证书以及由它们颁发给 SEGs 及 TLS 实体的证书列入 CRLs。同样，应保证将颁发给 SEG CA 及 TLS CA 的没有过期的交叉证书列入 CRLs。

为了恢复各个域之间的协同工作能力，运营商需要生成一个新的 SEG CA 或 TLS CA 密钥对并用它将证书颁发给运营商域内的所有 SEG 和 TLS 实体。该运营商应当发送交叉证书请求给双方之间有互连协定的运营商，来获取新的 SEG CA 或 TLS CA 密钥对。

建议运营商小心保护各自的 SEG CA 和 TLS CA 的密钥对，以此来限制对运营商团体的连锁效应。

5.2.8 SEG/TLS CA 证书更新

需要在旧的证书过期前更新 SEG CA 和 TLS CA 证书。SEG CA 和 TLS CA 证书的更新见 5.2.1 的交叉证书部分的描述。新 SEG CA 和 TLS CA 证书的更新过程应当在旧证书过期之前完成。

5.2.9 网络设备的注册

5.2.9.1 SEG 的注册

如果 SEG 证书没有创建，那需要创建一个 SEG 证书（5.2.11 具体描述了证书创建）。

如果新的 SEG 加入网络，那么需要用特定设备的管理方法来配置该 SEG 的策略数据库。

需要将该新 SEG 告知给其它运营商：其它网络的 SEG 策略数据库可能需要（与该新 SEG 策略数据库）符合。

5.2.9.2 TLS client 的注册

如果 TLS client 证书没有创建，那需要创建一个 TLS client 证书（5.2.11 具体描述了证书创建）。

如果新的 TLS client 加入网络，需要配置一些本地配置数据来使该新 TLS client 建立运营商之间的安全通信。另外，可以将该新 TLS client 告知给其它运营商。

5.2.9.3 TLS server 的注册

如果 TLS server 证书没有创建，那需要创建一个 TLS server 证书（5.2.11 具体描述了证书创建）。

如果新的 TLS server 加入网络，需要配置一些本地配置数据来使该新 TLS server 建立运营商之间的安全通信。另外，可以将该新 TLS server 告知给其它运营商。

5.2.9.4 NE 的注册

如果 NE 证书没有创建，那需要创建一个 NE 证书（5.2.11 具体描述了证书创建）。

如果新的 NE 加入网络，那么需要用特定设备的管理方法来配置该 NE 的策略数据库。

5.2.10 网络设备的注销

5.2.10.1 SEG 的注销

如果 SEG 从网络中移除，应该用特定设备的管理方法来移除 SA。该 SEG 的运营商应当将 SEG 证书列入到其 CRL。合作网络的 SPD 需要与该网络的 SPD 相符合。

5.2.10.2 TLS client 的注销

如果 TLS client 从网络中移除，应该用特定设备的管理方法来终止 TLS connections。该 TLS client 的运营商应当将 TLS client 证书列入到其 CRL。

5.2.10.3 TLS server 的注销

如果 TLS server 从网络中移除，应该用特定设备的管理方法来终止 TLS connections。该 TLS server 的运营商应当将 TLS server 证书列入到其 CRL。

5.2.10.4 NE 的注销

如果 NE 从网络中移除，应该用设备相关的管理方法来移除 SA。该 NE 的运营商应当将该 NE 证书列入其 CRL。

5.2.11 网络设备证书的创建

使用特定设备的管理方法，可发起证书创建。如 7.2 所规范的，可以用 CMPv2 协议来自动注册证书，或者使用 PKCS#10 格式来手动安装证书。这是运营商自己的决策，如依赖于 NE、SEG 及 TLS 实体的数量。

5.2.12 网络设备证书的撤销

如果 SEG 或 TLS 实体密钥对受到威胁，那么应当用特定设备的管理方法来移除现有的 SAs。该 SEG 或 TLS 实体的运营商应将该撤销的证书列入其 CRL。

5.2.13 网络设备证书的更新

新的 NE、SEG 或 TLS 实体证书需要在旧证书过期之前就位（更新）。该步骤类似于创建证书的步骤，可以如 7.2 所规范的使用 CMPv2 协议来自动注册证书，或者使用 PKCS#10 格式来手动安装证书。这是运营商自己的决策，如依赖于 NE、SEG 及 TLS 实体的数量。

5.2.14 NE CA 的注销

如果 NE CA 从网络移除,那么应保证将没有过期的 NE CA 证书及所有 NE CA 颁发给 NE 的证书列入到 CRL。

5.2.15 NE CA 证书的创建

NE CA 证书无需是运营商的顶级 CA,这意味着该 NE CA 不是自签名的。如果 NE CA 证书是自签名的,那么它们应该被安全地传递给运营商的每个 NE 并存储在其安全存储器中(参照 7.5 注释)。

注:创建 NE CA 证书与其它运营商没有关系。

5.2.16 NE CA 证书的撤销

这一严重事件要求撤销所有的 NE 证书。

不需要拆毁现有安全域内的安全连接,除非它们最近才形成,即:在运营商发现 NE CA 密钥受到威胁之后,但在证书被撤销列入 CRL 之前。

应保证将没有过期的 NE CA 证书及所有 NE CA 颁发给 NE 的证书列入到 CRLs。

为了重建安全域内的安全,运营商需要创建一个新的 NE CA 密钥对,并用其颁发证书给运营商自己域内的所有 NE。

注:撤销 NE CA 证书与其它运营商没有关系。

5.2.17 NE CA 证书的更新

NE CA 证书需要在旧 NE CA 证书过期之前得到更新。

注:更新 NE CA 证书与其它运营商没有关系。

6 配置

6.1 证书配置

注:本章包括一般的 3GPP 证书特性。本条款的一些部分也适用于其它标准中规范的设备及网络节点。涉及证书的新标准应当尽可能地参考本证书配置。

本标准描述了用于 NDS/AF 的证书。NDS/AF 构成部分不应期望获得其它实体的特别行为,这些特别行为基于本章规范外的证书域。

除了 IETF RFC 5280 中包含的要求外,还应该应用本标准中的证书配置的要求。这些要求适用于 SEG、NE、TLS 实体、SEG CA 及互连 CA。

在执行任何证书签名请求前,NE CA、SEG CA 及互连 CA 应当确保该请求符合本章中定义的证书配置。而且,CA 应当验证 Subject's DirectoryString 的顺序来检查连贯性,Subject's DirectoryString 属于其自身的管理域。

NE、SEG 及 TLS 实体应当验证证书应遵从 NDS/AF 特性,并应该只接受遵从了的证书。

6.1.1 证书的共同规则

——根据 IETF RFC 5280 规范的第三版证书。

——签名证书前使用的 Hash 算法:强制支持 SHA-1 和 SHA-256,禁止使用 MD-5 及 MD-2。出于安全,不推荐用 SHA-1 为新创建的证书做 Hash 运算。

注 1:为了与版本 9 之前的网元互通,某些时候证书中使用 SHA-1 是需要的。但是,在将来 3GPP 版本中,可能将禁止 SHA-1 用作证书 Hash 算法。

——签名算法:RSAEncryption。

——公钥算法: rsaEncryption。

——公钥长度至少应为 1024 比特, 推荐至少为 2048 比特。应当支持不少于 2048 比特的公钥长度。出于安全, 不推荐将公钥长度低于 2048 比特的公钥应用于新创建的证书。

注 2: 为了与版本 10 之前的网元互通, 某些时候证书的公钥长度低于 2048 比特可能是需要的。但是, 在将来 3GPP 版本中, 可能将禁止使用公钥长度低于 2048 比特的证书。

——CA 证书的公钥长度应当至少为 2048 比特, 并且应当支持至少 4096 比特长度的公钥。

——主体及颁发者名称帧。

——注意: C 是可选项: (C=<country>), O=<Organization Name>, CN=<Some distinguishing name>。

Organization Name 及 CN 应该在 UTF8 format 中。

或者,

——注意: ou 是可选项: cn=<hostname>, (ou=<servers>), dc=<domain>, dc=<domain>。

——应当支持 6.1a 规范的 CRL 来验证证书撤销状态。

——证书扩展在本标准中不是强制的, 但是在 IETF RFC 5280 提到了, 证书扩展对于具体实现是可选的。如果出现, 这样的扩展应当标记为“非重要(non critical)”。

6.1.2 互连 CA 证书配置

除了 6.1.1, 还需应用以下的要求:

——扩展:

——可选的非重要授权密钥标识;

——可选的非重要主体密钥标识;

——强制的重要密钥应用: 至少声明 keyCertSign 及 cRLSign;

——强制的重要基本限制: CA=True, path length unlimited 或至少 1。

6.1.3 SEG 证书配置

SEG 证书由 SEG 隶属的运营商域内的 SEG CA 直接签名。任何 SEG 应当用证书在 NDS/AF 中标明自己。

除 6.1.1 及 IETF RFC 4945 提供的信息外, 还应当应用以下的要求:

——颁发者名称与 SEG CA 证书中的主体名称一样。

——扩展:

——可选的非重要授权密钥标识;

——可选的非重要主体密钥标识;

——强制的非重要 subjectAltName;

——强制的重要密钥应用: 至少设置 digitalSignature 及 keyEncipherment;

——强制的非重要分布点: CRL 分布点。

注: 根据对等 SEG 间的 DNS 可用性, 需要应用以下规则:

- subjectAltName 应该包括 IP 地址 (如果 DNS 不可用);
- subjectAltName 应该包括 FQDN (如果 DNS 可用)。

6.1.3a TLS 实体证书配置

TLS client 证书应当由 TLS client 隶属的运营商域内的 TLS client CA 直接签名。TLS server 证书应当

由 TLS server 隶属的运营商域内的 TLS server CA 直接签名。

除 6.1.1 提供的信息外，还应当应用以下的要求：

——对于 SIP 域的证书，应该遵从 IETF RFC 5922、和 IETF RFC 5924 中的建议；

——颁发者名称与 SEG CA 证书中的主体名称一样；

——扩展：

——可选的非重要授权密钥标识；

——可选的非重要主体密钥标识；

——强制的重要密钥应用：至少设置 digitalSignature 及 keyEncipherment；根据 IETF RFC 5246，需要在 Diffie-Hellman 证书中设置 keyAgreement；

——可选的非重要扩展密钥应用：如果出现，至少为 TLS server 证书设置 id-kp-serverAuth，至少需要为 TLS client 证书设置 id-kp-clientAuth；

——强制的非重要分布点：CRL 分布点。

6.1.3b NE 证书配置

NE 证书由 SEG 隶属的运营商域内的 NE CA 直接签名。任何 NE 应当用证书在 NDS/AF 中标明自己。应用 6.1.3 所列的要求。

6.1.4 SEG CA 证书配置

除 6.1.1 提供的信息外，还应当应用以下的要求：

——主体名称与 SEG 证书中的颁发者名称一样；

——颁发者名称依赖于 SEG CA 颁发的证书的具体使用；

——如果用来建立拥有不同根 CA 的安全域间的互连通信，颁发者名称与互连 CA 证书的主体名称一样；

——如果用来建立与拥有 SEG CA 域中根 CA 证书一样的根 CA 证书的实体的连接，颁发者名称就是该根 CA 的主体名称，或者是拥有锁定该根 CA 的证书的中介 CA 的名称；

——扩展：

- 可选的非重要授权密钥标识；

- 可选的非重要主体密钥标识；

- 强制的重要密钥应用：至少声明 keyCertSign 及 cRLSign；

- 强制的重要基本限制：CA=True, path length 0。

6.1.4a TLS client/server CA 证书配置

除 6.1.1 提供的信息外，还应当应用以下的要求：

——主体名称与 TLS 实体证书中的颁发者名称一样；

——颁发者名称依赖于 TLS client/server CA 颁发的证书的具体使用；

——如果用来建立拥有不同根 CA 的安全域间的互连通信，颁发者名称与互连 CA 证书的主体名称一样；

——如果用来建立与拥有 TLS client/server CA 域中根 CA 证书一样的根 CA 证书的实体的连接，颁发者名称就是该根 CA 的主体名称，或者是拥有锁定该根 CA 的证书的中介 CA 的名称；

——如果用于不是由运营商 CA 颁发证书的 TLS clients，颁发者名称是运营商信任的根 CA 的主体名

称, 或者是拥有锁定运营商信任根 CA 的证书的中介 CA 的名称;

——扩展:

- 可选的非重要授权密钥标识;
- 可选的非重要主体密钥标识;
- 强制的重要密钥应用: 至少声明 keyCertSign 及 cRLSign;
- 强制的重要基本限制: CA=True, path length 0。

6.1.4b NE CA 证书配置

应用 6.1.4 中列出的要求, 但是对颁发者名称没有限制。

6.1aCRL 配置

— 根据 IETF RFC 5280 规范的第二版 CRL。

— 签名 CRL 前使用的 Hash 算法: 强制支持 SHA-1 和 SHA-256, 不应使用 MD-5 及 MD-2。出于安全, 不推荐用 SHA-1 为新创建的 CRL 做 Hash 运算。

注: 为了与版本 9 之前的基础部分相互协调工作, 某些时候 CRLs 中需要使用 SHA-1。但是, 可能在将来 3GPP 版本中, 将禁止 SHA-1 用作 CRLs 的 Hash 算法。

— 签名算法: RSAEncryption。

— 用来签名 CRL 的公钥长度至少应当与用来签名撤销的证书的公钥长度一样。应当支持 4096 比特长度的公钥来签名 CRL。

— 应当首先支持用 LDAPv3 的方法来获取 CRL。可以用 HTTP 来检验 TLS 和 NE 证书的撤销状态。

6.2 IKE 协商与配置

对于基于证书建立的 NDS/IP 元素之间的 IPsec SAs, 需要应用本标准中的 IKE 特性。是使用 IKEv1 还是 IKEv2 来协商 IPsec SAs 在 NDS/IP 规范中描述。

6.2.1 IKEv1 Phase 1 配置

除了 NDS/IP 规范的要求外, 需要应用以下基于证书的 IKEv1 认证的要求。

对于 IKE Phase 1 (ISAKMP SA):

- 应当支持用 RSA 来签名认证;
- 应当用 CERT 有用载荷 (包括网络设备证书) 的身份标识来做策略验证;
- 要求发起/响应网络设备在 IKE 消息中发送证书请求消息。

注 1: 至少应当发送一个空 CA 名称域的 CERTREQ 有用载荷来避免交互协调工作的问题。

- 对等 SEG 不应发送交叉证书, 因为交叉证书是预先配置在 SEG 中的;
- 网络设备应在最后 (第三条) 的 IKE Main Mode 消息的证书载荷中发送其证书;
- 证书载荷中的证书应当编码为 type 4 类型 (X.509 证书-签名);
- 应限制 Phase 1 IKE SA(ISAKMP SA)的生命周期至多为先到期的对端网络设备证书的剩余有效时间;

注 2: 根据对等网络设备间 DNS 的可用性, 需要应用以下规则:

- subjectAltName 及 ISAKMP 策略应包括 IP 地址 (如果 DNS 是不可用的);
- bjectAltName 及 ISAKMP 策略应包括 FQDN (如果 DNS 是可用的)。

6.2.1b IKEv2 配置

除了 NDS/IP 规范的要求外, 需要应用以下基于证书的 IKEv2 认证的要求。

对于 IKE_INIT_SA 与 IKE_AUTH 交互:

- 应当支持用 RSA 来签名认证;
- 应当用 CERT 有用载荷 (包括网络设备证书) 的身份标识来做策略验证;
- 要求发起/响应网络设备在 IKE_INIT_SA 交互消息中发送证书请求消息给响应者, 在 IKE_AUTH 交互消息中发送证书请求消息给发起者;

- 对等网络设备不应发送交叉证书, 因为交叉证书是预先配置在网络设备中的;
- 证书载荷中的证书应当编码为 type 4 类型 (X.509 证书-签名);
- 一旦网络设备的证书过期, 需要重新生成 IKE SA。

注: 根据对等网络设备间 DNS 的可用性, 需要应用以下规则:

- subjectAltName 及 IKEv2 策略应包括 IP 地址 (如果 DNS 是不可用的);
- subjectAltName 及 IKEv2 策略应包括 FQDN (如果 DNS 是可用的)。

6.2.2 交互协调工作的潜在问题

一些 PKI-capable 的 VPN 网关不支持 IKE 数据包的分割, 当在证书有用载荷中发送多个证书时, 需要强制 IKE 数据包分片, 这将会成为一个问题。这意味着直接交叉认证或手动引入对等 CA 证书到本地 SEG 并信任它对于桥 CA 系统来说是更优越的。当 IKE 在 IPv6 上运作时, 典型的 MTU 尺寸不会增加, 且长数据包还是需要被分割 (允许终端 UDP 掌控 IPv6, 见 IETF RFC 1981 中所述的 Path MTU Discovery for IPv6), 因此这将是潜在的交互协调工作问题。

一些 PKI-capable 的 VPN 网关支持 PKCS#7 做证书编码, 但是不应该用它。

6.2a TLS 配置

对于 3GPP 应用 TLS 来做运营商之间的安全, 应当应用本标准的 TLS 特性。

6.2a.1 TLS 配置

应满足以下要求:

- TLS server 应当在 ServerCertificate 消息中发送其网络设备证书;
- 如果 TLS server 要求, TLS client 应当在 Certificate 消息中发送其网络设备证书;
- 在 TLS 握手过程中, TLS 实体不应发送其交叉证书, 因为交叉证书在 TLS 实体中本地可用。

6.2a.2 交互协调工作的潜在问题

没有定义一般的潜在的交互协调工作的问题。

6.3 路径确认

6.3.1 路径验证配置

— 基于证书中 CRL 分布点, 应当用 6.1.1 所规定机制获取的 CRLs 来验证从对等网络设备那收到的证书的有效性。

— 基于证书中 CRL 分布点, 应当用 6.1.1 所规定机制获取的 CRLs 来验证从 TLS 实体那收到的证书的有效性。

— 任何 NE、SEG 或 TLS 实体应使收到的过期的对等实体证书无效, 但需要用一個否定结果来终止路径验证。

— 任何 NE、SEG 或 TLS 实体应使收到的 CRL 分布点域空的对等实体证书无效, 但需要用一個否定结果来终止路径验证。

— 证书有效性计算结果缓存在 SEG 或 NEs 中的时间, 不能超过 IKEv1 Phase 1 的生命周期, 或在使用 IKEv2 时不能超过网络设备所强制的生命周期。

— 证书有效性计算结果缓存在 TLS 实体中的时间不能超过 TLS 连接的生命周期。

7 架构与机制的详细描述

7.1 知识库

在安全连接建立期间, 任何一个网元、安全网关 SEG 或 TLS 实体, 都应根据 5.2.2 中所描述的内容来检查其对端实体证书的合法性。任何证书如果被撤回了(或者被一个新的证书所取代), 或者是一个网元 NE、安全网关 SEG、TLS 实体或运营商将证书注销了, 那么该证书都将无效。

考虑在网络 A 中的实体 A 与网络 B 中的实体 B 之间建立安全连接时, 实体 B 将进行如下检查:

- a) 实体 A 的 CA_A 的交叉证书有效。
 - b) 实体 B 的证书有效。
 - c) 获取 CA_A 实体 A 的交叉证书(如果不能在实体 A 的 cache 缓存或者本地存储中找到的话)
- 实体 A 从自己的角度执行相同的检查。

检查 a) 的执行可以通过询问本地的 CRL; 对于检查 b), 将需要询问实体 A 的 CA_A 的一个 CRL。在此时, 安全连接还不可用, 那么, 实体 A 的 CA_A 的公共 CRL 的获取将不通过安全连接进行。

图 4 和图 4a 所示为知识库(repositories)和以上提到的检查步骤 a)~c)。本地证书知识库(Certificate Repository (CR)), 包括了 SEG CAs 的交叉证书和可能的 TLS CAs 的交叉证书, 如果这些在 TLS 实体本地没有存储的话。本地 CRL (Local CRL) 包括 SEG CA 和 TLS CA 的交叉证书的撤回, 公共 CRL (public CRL) 包括了 SEG、TLS 实体、SEG CA、TLS CA 的证书的撤回, 并且能够被其他的运营商访问。

如果 NE 和 NE CA 的撤销信息没有包括在公共 CRL 仓库时, 它们可能包括在一个运营商的内部仓库(internal repository) 中。

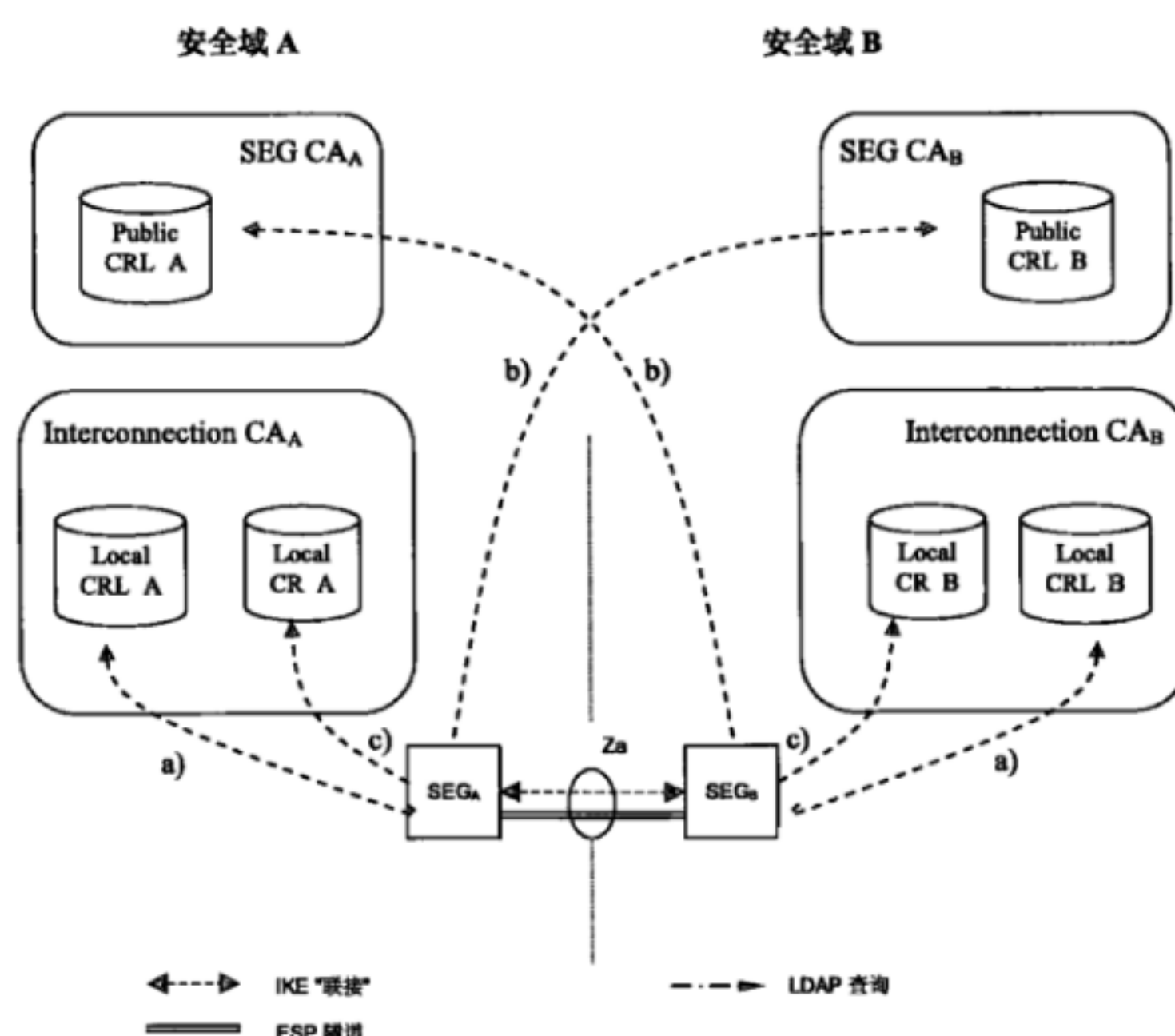


图 4 支持 Za 接口的 NDS/IP 的知识库

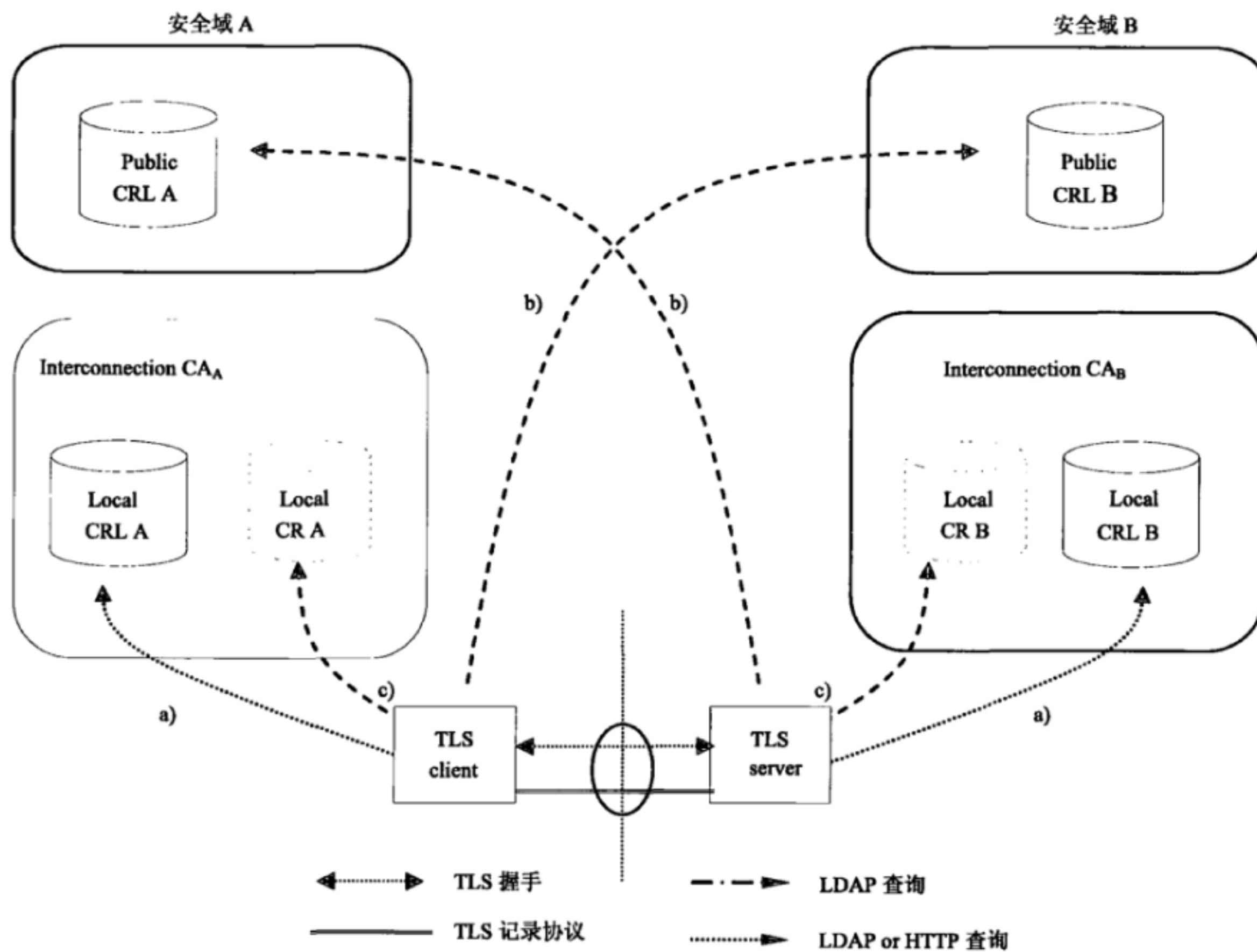


图 5 TLS 情况下的知识库

安全域 A

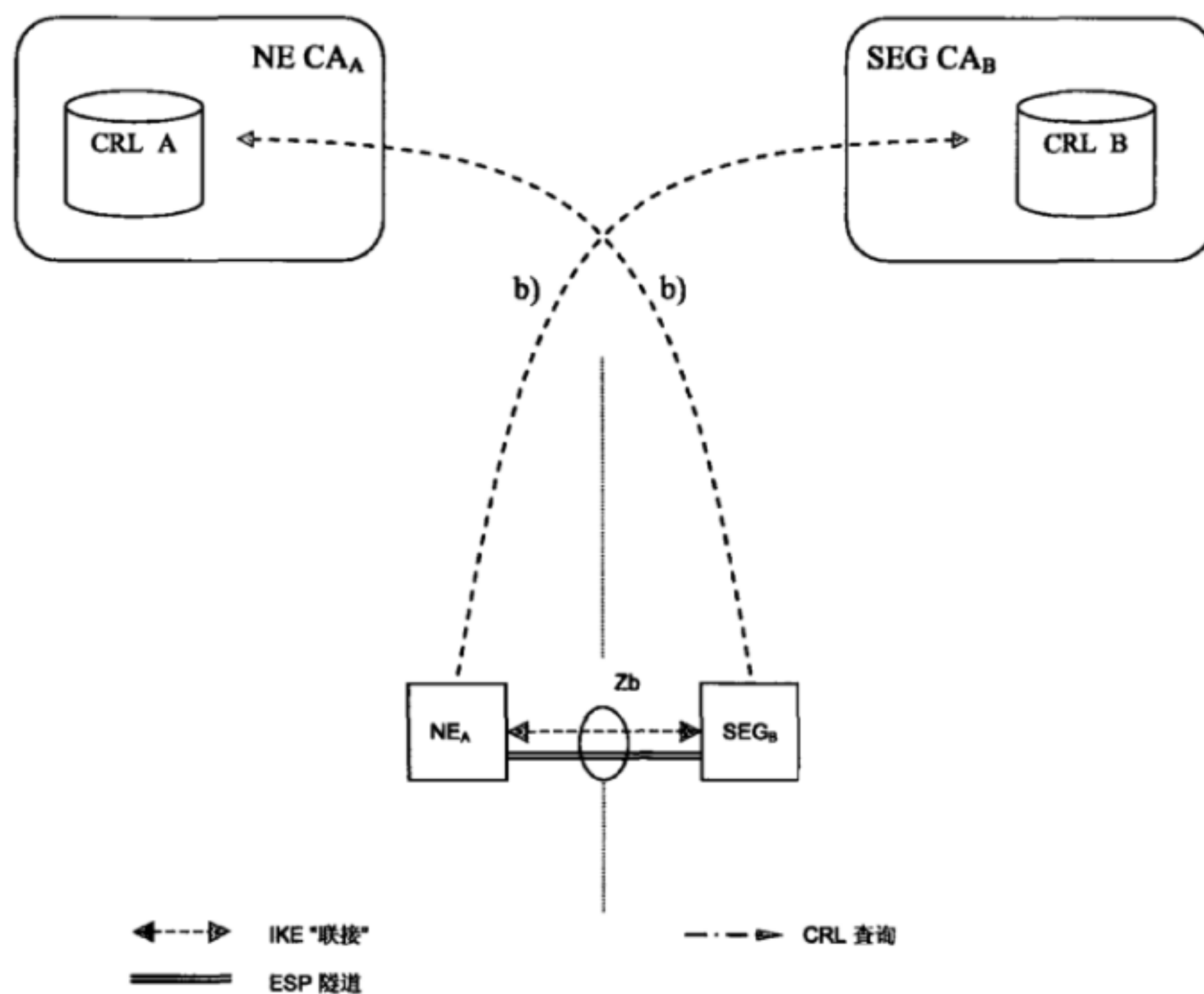


图 6 支持 Zb 接口的 NDS/IP 的知识库

如果 SEG CA 或者内部互联的 CA 被结合起来,那么公共的和本地的 CA 知识库,可能被作为独立的数据库或者单独的数据库来应用,作为单独的数据库时是具有两个不同接口的数据库。接入到“public”CRL 要根据网络内部的互联传输 (GRX) 进行。公共的 CRL 需要得到充分的保护 (例如:可以通过使用防火墙),同时公共 CRL 的拥有者也可以根据一些内部连接的协议来限制对公共 CRL 的访问。接入到 CRL 数据库不需要进行保护。

注 1: 首先,安全地接入到 CRL 数据库是不需要的,因为得到的 CRL 是被完整性保护的,并不包含任何的机要信息。其次,在当前没有任何可用的有效安全连接存在时,通过没有受到保护的接口接入公共 CRL 数据库是必须的。

安全网关 SEG 应使用 LDAP 接入 CRL 和交叉证书知识库。TLS 应使用 LDAP 或 HTTP 接入到 CRL 知识库。当交叉证书没有在 TLS 实体的本地进行保存时,TLS 实体可使用 LDAP 接入到交叉证书知识库。NEs 可使用 LDAP 或 HTTP 接入到 CRL 知识库。

注 2: 查找数据的接口 a) 和 c) 被用来建立运营商之间的安全连接,它们属于 NDS/AF (也包括 public b) 接口) 的范畴。目的是为了保证不同 SEGs、TLS 实体和知识库应用 (repository implementation) 的互操作。包括一个桥 CA 的交叉证书的可能的移动,也将要求对这些接口进行详细说明。

7.2 生命周期管理

IETF RFC 4210 中的证书管理协议 (CMPv2) 应支持对应的协议,以为 SEGs 提供证书生命周期管理能力。所以 SEG 和 SEG CA 应支持通过 CMPv2 的 SEG 向 SEG CA 的初始注册,例如:从 SEG CA 处获取证书,在证书过期之前通过 CMPv2 更新证书的密钥。

IETF RFC 4210 中的证书管理协议 version2 (CMPv2) 将支持对应的协议,以为 TLS 实体提供证书生命周期管理能力。所有的 TLS 实体以及 TLS CA 都将支持通过 CMPv2 进行的 TLS 实体向 TLS CA 的初始注册,例如:从 TLS CA 获取证书,在证书过期之前通过 CMPv2 协议更新证书的密钥。

IETF RFC 4210 中的证书管理协议 version2 (CMPv2) 应支持对应的协议,以为 NE 提供证书生命周期管理能力。所有的 NE 以及 NE CA 都应支持通过 CMPv2 进行的 NE 向 NE CA 的初始注册,例如:从 NE CA 获取证书,在证书过期之前通过 CMPv2 协议更新证书的密钥。

向 SEG、NE、TLS 实体注册证书时一个时常在运营商之间进行的交叉证书的过程,因此,相比起 PKC#10 方法,运营商需要更加自动的方法。然而,使用手动的安装 SEG 和 NE 证书的 PKC#10 形式也应当被支持。需要注意的是,SEG CA 交叉证书的生命周期相比起 SEG 证书的生命周期是很长的。

注:相对于已经被替代的 IETF RFC 2510 中定义的 CMPv1 而言,CMPv2 更加受欢迎,因为 CMPv2 与 CMPv1 可以互相协同工作。

7.3 交叉证书

双方运营商都使用以下的方法来产生 SEG CA 或 TLS CA 交叉证书:

- a) SEG CA 或 TLS CA 产生一个 PKC#10 证书请求,并将其发送给另一个运营商。
- b) 相互连接的 CA 从其他的运营商接收到相似的请求。
- c) 互相连接的 CA 接受请求,并产生一个新的交叉证书。

d) SEG CA 交叉证书存储在互相连接的 CA 的本地的 CR 上,并且使用 LDAP 来取得交叉证书。TLS CS 交叉证书可能存储在互相连接的 CA 的本地 CR 上,并且使用 LDAP 来获取交叉证书。另一种方法是,TLS CA 交叉证书可能存储在本地的 TLS 实体内部。

7.4 废除 SEG/TLS CA 交叉证书

以下过程用来撤回一个 SEG CA 交叉证书:

- a) 交叉证书被添加到互联的 CA 的 CRL 中。
- b) 交叉证书从 CA 的 CR 中被删除。

以下过程用来撤回一个 TLS CA 交叉证书:

- a) 交叉证书被添加到互联的 CA 的 CRL 中。
- b) 如果 TLS 交叉证书存储在互联的 CA 的 CR 中, 则交叉证书被删除。
- c) 如果 TLS CA 交叉证书存储在本地的 TLS 实体中, 则本地存储的交叉证书在 TLS 实体中被删除。

7.5 在 NDS/IP 端实体之间 Za 接口上使用 IKE 建立安全连接

在 IKEv1 的 Phase1 进行基于证书的认证, 或者在 IKEv2 IKE_INIT_SA/IKE_AUTH 交换, 如图 4 所示。SEGa 使用以下方法来认证 SEGb:

- a) SEGa 使用 CERTREQ 有效载荷, 请求 SEGb 的证书;
- b) SEGa 从 CERT 有效载荷中接收 SEGb 的证书;
- c) SEGa 认证 SEGb (检查签名);
- d) 如果本地存储的 CRL 过期了, 那么 SEGa 将从 SEG Cab 的 (公共) CRL 数据库取得 CRL;
- e) SEGa 使用这个 CRL 检查 SEGb 证书的状态;
- f) SEGa 使用本地存储的交叉证书或从互联的 CA 的 CR 中获取的交叉证书来检查 SEGb 的证书;
- g) 如果本地存储的 CRL 过期了, SEGa 将从本地互联的 CA 的 CRL 获取一个 CRL;
- h) SEGa 使用这个 CRL 检查 SEG CA 交叉证书的状态;
- i) SEG A 为运营商 B 的 SEG CA 检查交叉证书, 使用运营商 A 的互联的 CA 的证书。如果互联的 CA 不是最高级的 CA, SEGa 将检查互联的 CA 证书的状态, 否则, 互联的 CA 是隐含的可信的。

注: 如果本地 SEG CA 的公钥是安全的安装在运营商域中的每一个 SEG 上的, 那么, 当 SEGa 和 SEGb 属于同一个运营商网络时, 交叉证书的检查是不需要的。

7.5a 使用 TLS 建立安全连接

使用 TLS 建立安全连接的过程在 5.2.2 中进行了说明。

7.5b 在 NDS/IP 实体之间 Zb 接口上建立安全连接

在 Zb 接口上使用 NDS/IP 建立安全连接的过程在 5.2.2 中进行了说明。

7.6 CRL 管理

适用 NDS/AF 的 SEG 和 NE 不应发送 ISAKMP CERTREQ, 在这个消息中证书的类型为“证书撤回列表”。接收到该消息的 NE 和 SEG 可能忽略这个请求, 如 6.1.3 中说明的, CRL 应通过一个 CRL 分发点 (CRL Distribution point) 取回。

CRL 发布者 (很多情况下是 CA) 应只发放完整的 CRL 列表。delta CRL 的使用是不允许的, 因为可能存在的互相协调工作问题, 也因为在 NDS/AF 环境中不希望 full CRL 变得太大。完整 CRL 应只包括在 NDS/AF 中使用的被撤回的证书。在没有撤回的证书的情况下, CRL 发布者应当发布一个 CRL。如果一个存储的 CRL 还可用和有效时, SEG、NE、TLS 实体并不负责通过 CRL 分发点请求一个 CRL。如果没有有效的存储的可用的 CRL 时, NE、SEG、TLS 实体应当去获取一个 CRL。如果没有获得有效的 CRL, NE、SEG、TLS 实体应将其视为一个错误, 并取消隧道连接。

8 对于 NDS/IP 网元和安全网关的后向兼容性

网络域安全/IP 网络层安全(NDS/IP) 的规范 3GPP TS 33.210 描述了认证框架, 其中的初始 IKEv1/IKEv2 认证是基于预共享密钥(PSK)认证方式。NDS/AF 描述了一个可选的认证架构, 其中 NDS/IP 端实体 (NE, SEG) 能够执行基于 RSA 签名认证方法的初始 IKEv1/IKEv2 认证。一个支持 NDS/AF 的端实体也应包含 NDS/IP 功能。然而, 一个支持 NDS/IP 的端实体将并不需要包含 NDS/AF 功能, 除非进行了特殊的规定, 像 3GPP TS 33.210 或其他的规范中的情况。

专门的设备管理被用来重新配置一个网络设备, NDS/AF 功能在 IKE 发起者一端将被使用来进行初始的 IKE 认证 (例如: IKE Phase1 协商或者是 IKEv2 IKE_INIT_SA/IKE_AUTH 交换)。向基于 NDS/AF 的认证的转换可能由网络设备 (end entities) 来完成。在第一个 NDS/AF 端实体被启用之前, 它应能像 CR 一样, 确保所有需要的 NDS/AF 功能, CRL 数据库是可用的。基于 NDS/AF 的 IPsec 隧道的建立, 在与使用 PSK 认证方法对存在的业务量一起进行保护的同时, 能够被检测到。

一种平滑的移植可以按照 ([1]) 方式进行:

- 在 IKE 初始认证的过程中, 一个 NDS/AF 网络设备应提供多种算法, 其中的一些算法是基于 RSA 签名算法的, 其他的算法基于 PSK 认证方法。

- 如果对应的 IKE 对等实体不能支持 RSA 签名算法, 它将选择 PSK 认证方法。但是, 如果它依从 (支持) NDS/AF, 那么它将选择 RSA 签名算法。

- IKE 应答者策略 (IKE responder policy) 应被配置为, 使 RSA 签名认证方法比 PSK 认证方法具有更高的优先级, 以保证只要 IKE 发起者提议使用 RSA 签名认证方法, 则该方法应当被使用。

在各运营商之间 Za 接口上移动的情况:

如果两个运营商的 SEG 都支持基于 NDS/AF 的认证, 那么每个 SEG 的设置都将改变。预共享密钥可能在 SEG 上被移除, IKE 发起者应只使用 RSA 签名认证方法。然而, PSK 的移除并不是必选的, 它可能作为一种退却机制 (fallback mechanism) 来使用 (以保证认证的可靠进行)。需要注意的是, 不同运营商的 SEG 是同等的, 否则这可能导致隧道建立的失败。这种情况对应的就是, 如果初始的 IKE peer 只使用 RSA 签名认证方法, 并且对应的 IKE peer 只能接受 PSK 认证方法。此外, 如果引入 RSA 签名认证方法之后, 再将 PSK 作为一个退却机制进行保存, 那么只有在运营商改变 SEG 的策略并允许使用 PSK 时, 才会退而使用 PSK 认证方法。有时, 运营商也会临时允许退却到 PSK 方式, 例如, 由于 PKI 的问题, SEG 不能检查必要的证书。如果 PSK 被作为一种退却机制, 或者当怀疑 PSK 不安全时, 那么出于对安全的考虑, 周期性地更新 PSK 也是必要的。

9 基站的证书注册过程

9.1 概要

本章主要说明了回程链路安全的证书注册机制。对于是否应用本机制, 将由 3GPP 的其它规范和运营商来决定。

9.2 架构

图 7 所示为一个运营商 PKI 下基站证书注册的总体部署架构。

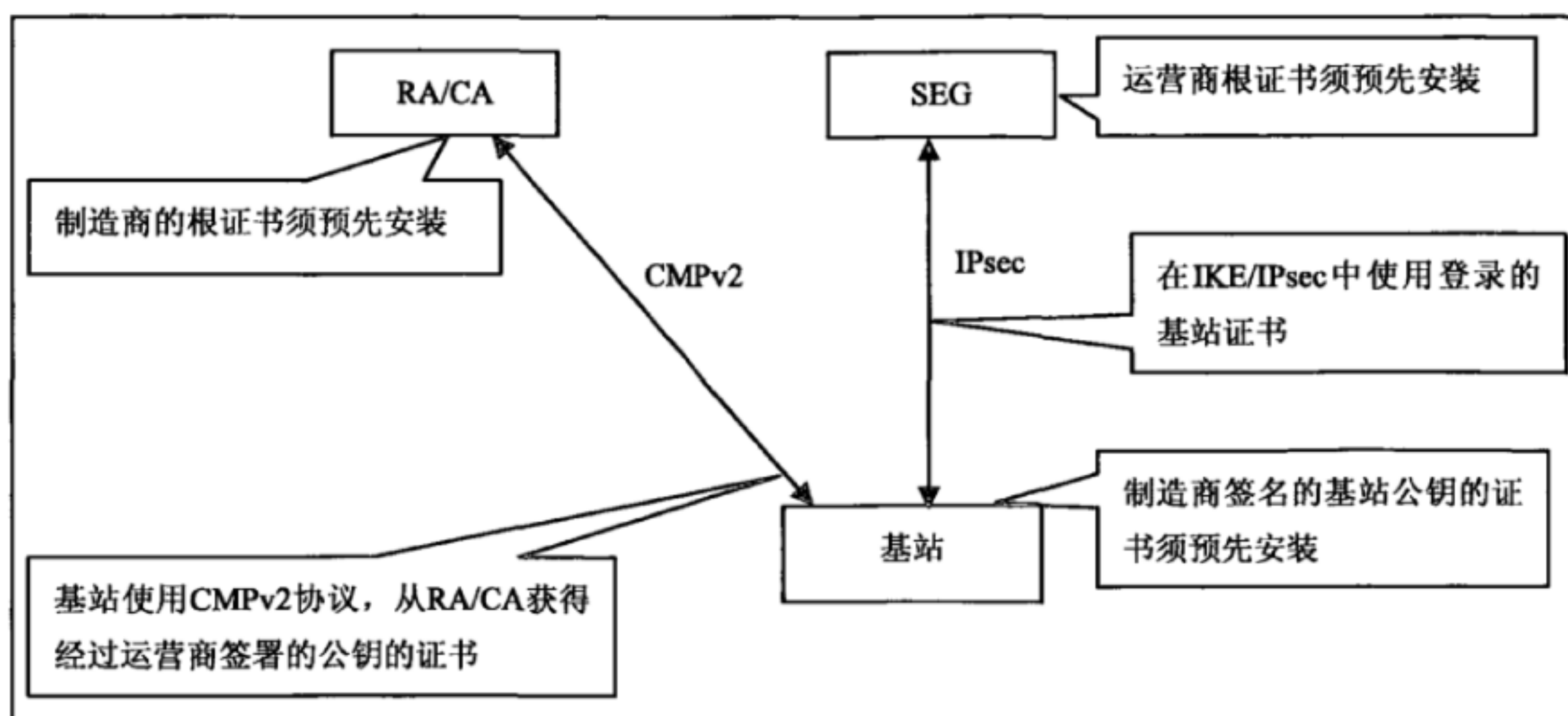


图7 安全架构总述

基站要由设备商预先提供一个公私密钥对，并且具有预置公钥的设备签名的证书。

在初始连接到运营商网络时，基站将与运营商的 RA/CA 之间建立通信的通道。使用 IETF RFC 4210 中的 CMPv2 时，一个对证书的请求将被发送到 RA/CA。网络认证从基站发来的消息，此认证主要是基于基站的有设备商签名的证书和预置在网络中的设备上的根证书进行的。基站应检查从 RA/CA 收到的消息的完整性，此检查是基于为基站提供的运营商的根证书进行的。在相应消息中，基站接受运营商签名的证书。在执行 CMPv2 协议的过程中，基站需要成功地提供一个关于拥有某一私钥的证明，而这个私钥与某一个公钥相关联是被认证的。

运营商根证书，可能在 CMPv2 协议执行时或执行之前被预置在基站中。在预置时对运营商根证书的保护根据运营商的安全策略来决定。如果在执行 CMPv2 之前提供了运营商的根证书，基站应当使用它。否则，基站应当使用在执行 CMPv2 过程中得到的运营商根证书。如果始终没有提供运营商根证书，基站将中断这个过程。

在注册过程结束之后，基站能够将运营商根证书用于运营商的 SEG 对它的认证，SEG 是预置有运营商根证书的。接着，基站将使用运营商根证书来认证 SEG。

注：向 SEG 的认证是 3GPP TS 33.210 中使用基于 IPsec 的回程链路安全的一部分。

如果在之后基站部署的阶段中，运营商想要更新基站的证书，那么运营商签名的旧证书将执行相同的步骤，取代在初始注册过程中设备商签名的证书。

9.3 安全机制

基站的注册过程应当使用如 IETF RFC 4210 和 IETF RFC 4211 中所述的 CMPv2 协议。也应当继续使用 IETF RFC 4210 中和 IETF RFC 4211 中所述的所有权证明方法（proof-of-possession method）。

用于基站注册过程的 CMPv2 的简要介绍在本标准的 9.5 中给出。

9.4 证书简介

9.4.1 概述

在基站注册过程中用到的所有证书都应遵循本标准第 6 章中的需求。例外的情况在以下的条中进行说明。

9.4.2 设备商根 CA 证书

设备商 CA 的根证书应遵循 6.1.2 中互联 CA 证书 (interconnection CA certificate) 的内容, 除了以下的例外情况:

- 证书中的 CRL 分配点扩展是可选的。
- 设备商将支持证书撤回信息的分发。提供撤回数据的接口不在本标准的范围之内。

9.4.3 设备商 CA 证书

如果设备商没有使用设备商根 CA 对基站证书进行签名, 由 CA 或者任何中间设备商 CA 对基站证书进行签名的证书都应遵循 6.1.4 中关于 SEG CA 证书的内容, 除了以下的例外情况:

- 发行者名将可以是任何的设备商 CA, 因为最后的证书链是从基站的证书开始直到设备商根 CA 的。
- 路径长度是大于 0 的, 因为中间的 CA 并不直接对设备商基站证书进行签名。
- 在 9.4.2 节规定的证书中 CRL 分配点扩展和证书撤回信息的分配将被应用。

9.4.4 设备商基站证书

由设备商 CA 进行签名的基站证书应遵循 6.1.3b 中关于 NE 证书内容的规定, 除了以下的列外情况。

- 发行者名是对基站证书进行签名的设备上 CA 名。
- 证书的 subject name 应是一个由设备商提供的全球唯一的完全合格的域名 (fully qualified domain name - FQDN)。因为设备商保证了全球的唯一性, 所以 FQDN 由设备商来进行准确定义。Subject name 的格式应遵从 6.1.1 中的内容, 使用不同的 o attribute 和 cn attribute, 其中 o attribute 应包含设备商名, cn attribute 应包含 FQDN。

- 包含了 dNSName 类型的 subjectAltName 应如同 subject field 一样包括相同的 FQDN。

注 1: 证书中的 FQDN 对于 DNS 的可用性是不要求的。

注 2: 例如: 设备商基站 FQDN 可以为 <serialnumber>.<vendor>.com。注意: 所有的标签都必须服从对 FQDN 中标签的要求 (参考: IETF RFC 1035)。在 subject field 中的表现可以为 "o = <vendor name>, cn=<serialnumber>.<vendor>.com"。

- 在 9.4.2 节规定的证书中 CRL 分配点扩展和证书撤回信息的分配应被应用。

9.4.5 运营商根 CA 证书

运营商根 CA 的根证书应遵循 6.1.2 中对于互联 CA (interconnection CA) 证书的内容。

9.4.6 运营商 RA/CA 证书

运营商可能为签名的证书和签名的 CMP 消息分别配置私钥, 或者为它们配置单独的私钥。因此 RA/CA 可能具有一个或两个证书。

用于证书签名的 RA/CA 证书应遵循 6.1.4 中 SEG-CA 证书内容的要求, 除了以下的例外:

发行者名为任何运营商 CA 的名, 因为最终的证书链是从 RA/CA 证书开始直到运营商根 CA 的。

用于 CMP 消息签名的 RA/CA 证书应遵循 6.1.3 中 SEG 证书内容的要求, 除了以下的例外:

- subject name 与用于证书签名的 RA/CA 证书名相同。

发行者名为任何运营商 CA 名, 因为最终的证书链是从 RA/CA 证书开始直到运营商根 CA 的。

如果运营商设置了单独的私钥用于签名基站证书和签名 CMP 消息, 对于单独的 RA/CA 证书应遵从上述的用于证书签名的 RA/CA 证书的要求, 同时还要增加如下内容:

除了 6.1.4 中说明的密钥应用扩展外, 还要强制进行 critical key usage extension bit (重要密钥应用扩

展比特) digitalSignature 的设置。

注: 根据普通的安全惯例, 推荐使用互相隔离的私钥和证书。

9.4.7 中间的运营商 CA 证书

如果运营商没有使用它的运营商根 CA 签名 RA/CA 证书, 并且如果 RA/CA 证书没有直接被运营商根 CA 签名, 那么所有中间的运营商 CA 证书应遵循 6.1.4 中关于 CA 证书内容的要求, 除了以下的例外情况:

- 发行者名是任何的运营商 CA 名, 因为最终的证书链是从 RA/CA 证书开始, 直到运营商根 CA 的。
- 路径长度将大于 0。

9.4.8 运营商基站证书

由运营商 RA/CA 签名的基站证书应遵从 6.1.3b 中关于 NE 证书内容的要求。

其他的文档可能会根据他们的部署场景, 规定不同的基站证书的内容。

注: 基站证书的扩展应用将可能与本标准中说明的对 NDS/AF 的 NE 证书的应用不相同。因此, 准确的内容应该取决于说明了扩展应用部署的场景。

9.5 CMPv2 简介

9.5.1 总体需求

在基站与 RA/CA 两端之间使用 CMPv2 协议时, 应遵循如下的要求:

— 本 CMPv2 简介只包含正式请求与密钥更新功能。撤回处理、PKCS#10 请求和 CRL 获取, 将不作为本 CMPv2 简介的部分。

— 对于 PKI 消息的保护, CMP 不会使用不对称算法, 在本标准范围内也不会使用 PasswordBasedMac。

— 基站应被预置公私密钥对(设备商密钥对)和相关的由设备商 CA 签名的设备商证书。

— 有存在一条由基站证书直到设备商根 CA 的证书链, 那么中间的证书也应提供给基站。

— 运营商根 CA 证书也可预置到基站中。

— 如果基站没有预置运营商根 CA 证书, 那么基站应从初始化响应中(initialization response)接收到的证书中获取运营商根 CA 证书。选择过程应基于检查哪个根证书能够被用来检查接收到的基站证书。

注 1: 运营商根证书的更新不在本条中基站注册的范围中。因此假设基站始终都有一个有效的运营商根证书可用于检查密钥更新响应。

— RA/CA 应对初始化请求进行认证, 认证是基于检查设备商根 CA 的签名进行的。

— RA/CA 应认证密钥更新请求, 认证过程是基于检查运营商根 CA 的签名进行的。

— RA/CA 中应配置有设备商根证书。如果在执行 CMPv2 协议的过程中, 基站中配置了运营商根证书, 那么 RA/CA 也将配置有运营商根证书。

— RA/CA 中应配置一个 RA/CA 证书, 这个证书是被运营商根 CA 或被运营商根 CA 下的中间的 CA 签名的。

— 如果 RA/CA 使用的是不同的私钥来签名产生的证书和 CMPv2 消息, 那么 RA/CA 应配置两个相关的证书, 例如: 用于证书签名的 RA/CA 证书, 和用于 CMP 消息签名的 RA/CA 证书。

— 如果 RA/CA 证书(或用于签名证书和签名 CMP 消息的私钥相互独立时)没有直接由运营商根 CA 证书进行签名, 那么中间 CA 的证书也应为 RA/CA 配置。

— 生成签名之前, 在 PKIMessage 的保护域 (protection field), 以及证明所有权 (proof-of-possession) 时使用的哈希算法和 6.1.1 中定义的用于证书签名的哈希算法是相同的。使用的签名算法应与证书相关内容中的相同。

证书方面的内容在 9.4 中说明。

注 2: 这些证书的内容隐含的说明了在以下小节中提到的证明所有权 (proof-of-possession) 和 PKIMessage 的不同的签名中使用的算法。

注 3: RA/CA 对证书的产生和分发表管理的策略不在本标准的范围内, 由运营商进行决定。

9.5.2 PKIMessage 特性

以下内容将被应用于 IETF RFC 4210 中所说明的 PKIMessage:

— 在本部分的内容中要求对于 PKI Protection 类型的可选保护域的支持和应用。基站中使用的消息特定的私钥 (message-specific private key) 在 9.5.4 中关于基站发送的请求的单 PKI 消息体 (single PKI message bodies) 部分的内容中进行了说明。对于 RA/CA, 应使用 RA/CA 私钥, 或者如果基站证书和 CMPv2 消息被不同的私钥签名, 那么应使用单独的 RA/CA 私钥对 CMP 消息进行签名。

— 本部分内容要求支持可选的 extraCerts 域。在这个域中的证书可能以任何的顺序排列, 这个域中消息特定的内容 (message-specific content) 在 9.5.4 中关于单 PKI 消息体部分的内容进行了说明。

— 在这部分内容中所有的 CMPv2 消息都应由一个 PKIMessage 组成, 例如: 在所有的情况下, 用于 PKIMessage 的序列号的大小为 1。

9.5.3 PKIHeader 域特性

以下内容将应用 IETF RFC 4210 中所述的 PKIHeader field 部分的内容。

— 发送者和接收者域 (sender and recipient fields) 应包含基站和 RA/CA 的身份标识。这些标识都应该与公钥的证书中的 subject name 一致, 该证书对应的私钥用于 PKIMessage 的签名, 如果发送者根据规则不知道接收者的身份, 则可使用任何一个发送者知道的名字。

— PKIMessage 中的 “protection” field 和 PKIHeader 中的 “protectionAlg” 是强制的, protectionAlg 为 MSG_SIG_ALG 类型的。签名算法应该基于签名者的证书 (属于基站或 RA/CA) 中 SubjectPublicKeyInfo 算法域所含的算法。在签名之前用于对 PKIMessage 做 Hash 运算的算法应该遵循 6.1.1 介绍的证书签名前的算法规范。

— transactionID 的使用是强制的, 并推荐使用 IETF RFC 4210 中给出的 transactionID 的处理过程。对于 transaction 中的第一条消息, 基站应设置这个域为至少 8 字节的随机数, 并在所有后续消息中使用同样的随机数。

— senderNonce 和 recipNonce 这两个域的使用是强制的。并应使用 IETF RFC 4210 中推荐的域长度。在 transaction 最早的消息中的 recipNonce, 应被发送者设置为 0, 且应被消息的接收者忽视。

9.5.4 PKIBody field 特性

9.5.4.1 概述

基站证书注册应支持以下 CMPv2 消息体:

- 初始化请求 (ir);
- 初始化响应 (ip);
- 密钥更新请求 (kur);

- 密钥更新响应 (kup);
- 确认 (pkiconf);
- 证书确认 (certconf)。

关于以上给出的单消息体的内容将包括在以下的子条中。如果没有特别的说明, 则使用 IETF RFC 4210 中和 3GPP TS 33.203 中的规范。

9.5.4.2 初始化请求

IETF RFC 4210 中所定义的初始化请求应包含 IETF RFC 4210 中和 IETF RFC 4211 中所定义的 CertReqMessage, 例如: 在所有的情况下, CertReqMessage 的序列大小为 1。

以下内容应当应用于 CertReqMessage 域和它的子域:

- 如果基站知道自己的建议使用名, CertTemplate 的 subject 域应包含基站的建议使用名, 否则应被省略。

- CertTemplate 中的 publicKey field 是强制性的且应包含被 RA/CA 鉴定的基站的公钥。为了执行 CMPv2 协议, 公私密钥对可被预置到基站中, 或在基站内部产生。这个域 (field) 的格式应遵循 IETF RFC 5280 中的规定。

注 1: 引用文件 IETF RFC 4211 对标准 IETF RFC 3280 中 publicKey field 的格式已经失效。本标准主要参考 IETF RFC 5280。

- CertReqMessage 应包含一个类型为 ProofOfPossession 的 POP 域。POP 域应包含一个 POPOSigningKey 类型的签名域。POPOSigningKey 域中的 algorithmIdentifier 域, 应包含一个基站用来产生 Proof-of-Possession 值的签名算法, 例如: POPOSigning 域中的签名。

- 如果 POPOSigningKey 类型的 poposkInput 域中的 POPOSigningKeyInput 域被使用了, POPOSigningKeyInput 中的 sender 域应是强制性的且应包含基站的身份标识。此标识是由生产基站的设备商提供的, 并包含在设备商提供的基站证书中。

注 2: 根据 IETF RFC 4211, 如果 CertTemplate 域中的 subject 域被省略, 那么 poposkInput 域是强制的。

注 3: 根据 IETF RFC 4211, 只有当发送者 (sender) 已经获得经过鉴权的身份, POPOSigningKeyInput 的 sender 域才会被使用。本标准假设发送者 (例如基站) 有制造商签名预置的合法证书, 所以发送者的身份可以认为是经过鉴权并确立的。

由基站发送的 PKIMessage 应被设备商提供的私钥签名。

承载了初始化请求的 PKIMessage 中的 extraCerts 域应是强制的并应包含设备商提供的基站证书。如果基站证书没有被设备商根 CA 签名, 那么直到设备商根证书 (的证书连) 的中间证书也都应包含在 extraCerts 域中。

9.5.4.3 初始化响应

如 IETF RFC 5280 中所述的初始化响应应该包含一个基站证书, 例如: 在所有情况下, CertResponse 的顺序 (队列) 的大小应为 1。

以下内容应该应用于 CertRepMessage 域和它的子域。

产生的证书应被传送到基站, 在 CertResponse 域中的 certfieldKeyPair 域中。传送的过程不可以被加密 (即, CertorEncCert 中的证书域应是强制的)。

承载了初始化响应的 PKIMessage 中的 extraCertts 域应是强制的并应包含运营商根证书和 RA/CA 证

书（或多个证书，如果证书签名和 CMP 消息签名使用的是相互分离的证书时）。如果 RA/CA 证书没有被运营商根 CA 证书签名，那么直到运营商根证书的证书链的中间证书应被包含在 extraCerts 域中。

9.5.4.4 密钥更新请求与密钥更新响应

这些消息的形式和内容与初始化请求与响应消息是一致的，因此在前面的条中关于初始化请求和初始化响应的内容可以一样的应用，除了以下的例外：

- 由基站发送的 PKIMessage 应被私钥进行签名。此私钥是关联于上次接收到的运营商提供的基站证书的。extraCertsField 应是强制的并应包含与用于 PKIMessage 签名的私钥关联的基站证书。如果基站证书没有直接被根 CA 签名，那么应包含任何的中间证书。

9.5.4.5 证书确认请求和确认响应

初始化响应和密钥更新响应应当始终跟随着一个证书确认请求和确认响应消息的交换。

基站发送的 PKIMessage 应被同一个私钥进行签名，这个私钥被用在前述的初始化请求或密钥更新请求中。

承载着证书确认请求和确认响应的 PKIMessage 的 extraCerts 域应被省略。

9.6 CMPv2 传输

在网络设备和 RA/CA 之间 CMPv2 消息的传输应使用基于 HTTP 的协议进行，正如 IETF RFC 6712 中说明的。

应支持网络设备（end entities）发起的通信，其中每一个 CMP 请求消息触发一个从 CA/RA 的 CMP 响应消息。而对于 RA/CA 发起的 HTTP 请求（如：宣告）的支持不是必需的。

注：CMP 提供内置的完整性保护以及鉴权。对于根据 IETF RFC 2818 的 TLS（HTTPS）之上 HTTP，或者 VPN 的可选使用，参照 IETF RFC 6712。

附 录 A
(规范性附录)
重要和非重要的证书扩展

根据 IETF RFC 5280 的 4.2 节, 可以指明一个证书扩展是重要或者不重要的。

“如果一个使用系统 MUST 的证书遭到一个它不认可的重要扩展, 它会拒绝认证。但是, 如果它不被认可, 可能会忽视一个不重要的扩展。”

关于执行需求, 可做可选的和强制的支持声明。一个正在接收的 SEG 或者 TLS 实体应能处理一个标记为重要的扩展, 这个扩展在 NDS/AF 中是强制支持的。当是可选的支持时, 根据 IETF RFC 5280, 一个收到的、标记为重要的扩展将导致一个错误。

附 录 B

(资料性附录)

对简单信任模型的决定

B.1 前言

为了证明对需要手动交叉认证的“简单信任模型”的决定，本节讨论两个基本方法的技术优点和缺点，这两个基本方法出于漫游流量保护的目，为运营商间提供信任，即交叉认证和桥 CA。桥 CA 是一种交叉认证方法的扩张，且在 NDS/AF 可行性研究 (3GPP TR 33.810) 中被视为是为运营商间提供信任的、值得推荐的可行性解决方案之一。考虑到目前 PKI 软件的状态和有选择时对简单解决方案的一般需要，会为 NDS/AF TS 选择没有桥 CA 的交叉认证。本附录讨论这种指导的背景动机。

没有桥 CA 模型的直接交叉认证和目前在因特网 IPsec 世界的实践有很强的关联，在因特网 IPsec 世界里，为每一个 IPsec 连接都配置一个受信任的 CAs 的列表，并且任何携带有证书的人都允许接入，此证书有一个到这个受信任的 CA (信任锚点) 的信任路径。在这种模型中，在达成漫游协议时就已进行了交叉认证。这被称之为“简单信任模型”。

桥 CA 模型假设，出于被其他运营商鉴定的目的，所有愿意和其他运营商建立漫游协议的运营商首先会被桥 CA 认证。这是一个必需的预备步骤。下一步，当已经达成了漫游协议，运营商将给他们的 IPsec 隧道配置这样的信息，即在这些能够确认的运营商 (这些运营商有桥 CA 颁发的一个证书) 中哪一个运营商能使用这个 IPsec 隧道。这称之为“扩展的信任模型”，或者“独立信任和接入控制”。

本附录不讨论证书对预共享密钥的好处。交叉认证对漫游同等 CAs 清晰的列表的好处，包括这个更简单的、通往一个可能的最终桥 CA 模型的演变路径。

B.2 NDS/AF 中信任模型的需求

以下是对 NDS/AF 信任模型的一个需求列表。

A. 部署的简单性和容易性。当运营商在网络配置中需要隧道流量时，PKI 带来很多好处，但是它的应用不应该受一个不必要的复杂技术解决方案的阻碍。对于和另一个运营商交换流量必要的、需要的、技术性的且合法的操作应该尽可能简单直接。

B. 和现存标准的兼容性。为什么现存的 PKI 标准应该扩展以适应 3GPP 环境，对于这个问题除非有明确的需求，否则，3GPP 规范应该适应现有标准。这允许运营商有最好的设备选择，且允许与非 3GPP 环境相互协作。

C. GRX 和非 GRX 运营商都可用。使用 GRX 的供应者的和不使用 (使用租借的线，或者甚至市公共因特网) 的运营商应该能够使用 NDS/AF 方法来安全的交换流量。

B.3 交叉认证方法

B.3.1 手动交叉认证

这句话刻划了手动交叉认证的信任模型：“除非明确允许，否则不信任任何人”。为受信任的授权颁发一个证书，产生了允许。手动交叉认证很容易理解。同样的，其安全只依赖于在本地所做的决定。

B.3.2 有桥 CA 的交叉认证

这句话能刻划 bridge-CA 的信任模型：

— “除非明确否定，否则信任每一个 Bridge-CA 信任的人”。明确的否定可以通过给 bridge 颁发的证书写限制来处理。

— “信任我颁发给 bridge 的证书上列出的任何人”。明确的允许列出在颁发给桥（以名字约束的形式）的证书上。

对于 X.509 证书，命名约束是一种很少使用的扩展。本质上，它是一个基于证书上的命名来明确信任谁或者不信任谁的条款。相对来说很少使用它们的事实和很少有关于它们的正式文档的事实都是一个冒险。命名约束也需要一些组织能够做命名注册，从而避免命名冲突。

B.4 桥 CA 方法的问题

B.4.1 证书的命名约束支持或者法律严格绑定和审查的需求

如果没有防范，即使没有授权，已经由桥 CA 签署其 SEG CA 的运营商（M）产生与另一个运营商（A）的证书相似的证书是可能的，并让 M 接入到运营商（B）的网络。

我们说运营商 B 在接入它预留的用以处理漫游流量的子网时，有如下的配置：

- 本地子网络=一些 IPv6 子网络地址；
- TrustedCA's = BridgeCA；
- AllowedCertificateSubject = O=Operator A or O=Operator C or O=Operator D。

注：远程 SEGs 的 IP 地址是不受限制的，当完成了基于证书的认证，并且允许所有受信任的运营商相似接入。假如不同的国外运营商需要接入不同的子网络，将会有多个与上面相似的配置块，附带有恰当说明的 IP 地址。

具有 PKI 能力的 IPsec 设备，广泛支持这种“AllowedCertificateSubject”特性（术语名称非实际存在）。假如运营商 M 为它的证书使用以下形式的证书，将不会被允许接入：

- Subject: CN=SEG 1, O=Operator M；
- Signer: CN=SEG CA, O=Operator M。

然而，它可以虚构以下格式的证书：

- Subject: CN=SEG 1, O=Operator A；
- Signer: CN=SEG CA, O=Operator M。

使用这样的证书会允许完整的但却非法的接入到运营商 B 的网络中，这个网络显示运营商 A 在使用。现在，有以下的可能来规避这个问题：

- a) 在认证外国运营商时，也检查签名者的命名，可以通过两种方法：
 - 1) 一个拥有的“允许的证书签名者”的特性；
 - 2) 为运营商 M 颁发的桥 CA 证书中的命名约束提供支持。
- b) 建立强大合法的捆绑和审查，这些捆绑和审查将使运营商 M 避免运营商 A 证书的非法虚构。

方案 a, 1) 的问题是，现有 PKI 末端实体产品一般不会支持这种“允许的证书签名人”，这和需求 B 存在冲突。

方案 a.2) 的问题是，现有 PKI CA 或者末端实体产品一般不会支持这种证书中的“命名约束”特性，这和需求 B 存在冲突。

方案 b 的问题是，首先，在任意一对运营商能利用 NDS/AF 机制交换漫游流量前，应找到一个愿意运行桥 CA 的组织。其次，应当有建立的文书工作和审查流程来确保能够发现在此描述的业绩。这和需求 A 存在冲突。同样的，不能在技术上提前阻止所描述的非法行为。

如果使用命名约束，当每次达成一个新的漫游协议时，每一个运营商应更新其颁发给 Bridge 的证书，在证书里增加新的漫游伙伴的命名。从一个运营商的角度来看，不管在使用桥 CA 还是直接的交叉认证模型，用于签名操作的新证书的数量是一样的。

B.4.2 阻止命名冲突

如果用命名约束来防止额外的涉及桥 CA 的“管理机构”，那么写在证书里的命名需要和一个第三方注册，以防止两个运营商意外的或者故意的在他们的证书里使用相同的命名。这和需求 B 存在冲突。

B.4.3 建立信任时所需的两个多余的步骤

正如前言里所描述的，附带着“扩展的信任模型”，首先通过桥（认证）认证每一个运营商，然后，在配置 IPsec 隧道（接入控制）时列举信任的运营商。

对于使用的桥 CA 模型，需要有一个所有其他参与方都能信任的组织，且这种信任应是传递的！如果你信任桥，你也应该信任其他通过交叉认证连接这个 bridge 的组织。如果运营商 A 和桥 CA 相互交叉认证，运营商 A 将自动信任所有其他已经鉴定的且服从规则的运营商。而且这种信任和漫游流量隧道无关，此隧道的配置应独立于 PKI。

因此，在使用交叉认证时，即使避免了在 SEGs 中配置新证书，漫游信息也会通过安全网关一些其他的方式来配置和维持。而其困难的部分是：PKI 提供的信任和漫游协议如何结合？因为在这种情况下 PKI 提供的信任和漫游协议是不同的。

需要两个步骤：

步骤 1) 通过桥 CA 建立“信任”=>认证对等的 SEG；

步骤 2) 在隧道配置中，详细说明哪一个出现的对等的 SEGs 可以信任。

如果没有通过桥 CA，交叉认证就完成了，那么这两步可以合二为一。如果无论如何都要限制对等的 SEGs，那么 PKI 提供的信任（步骤 1）的附加值是什么？

B.4.4 IKE 执行相关的长证书链

如果使用 Bridge A，除本地末端实体（SEG）证书外，在证书有效负载内，应发送一个 SEG CA 证书，这导致以太网环境中 IKE 包的分裂，一些现有 IKE 不支持这种分裂。它是实现上的一个问题，而不是协议的问题。即使在 IPv6 中，也需要分隔 IKE UDP 包，这造成一个潜在的协同工作能力的问题。清楚的是，使用一个不同的协议并不是一个解决方案，但是取而代之的是，应该固定现有实现。尽管如此，考虑到需求 B，通过不强制分裂 IKE 包来完全避免这个问题是更安全的，这些 IKE 包的分裂是通过不使用桥 CA 而得到的。

B.4.5 现存相关桥 CA 经验的缺乏

在美国，联邦 PKI 是一个样品部署，在这个样品部署中，桥 CA 用来将不同的联邦代理的 CA 连接在一起。然而，即使在联邦政府组织内，它似乎是唯一的备有证明文件的一种，并且与沉重的政策文件和十分沉重的审查实践有关。在这种情况下，批准使用桥的方法，因为他们希望自动检查一些实体是否有合法的权力签署一些文件。使用交叉域 PKI 有效的实体的数量可能是数百万个，而且对于一个有效实体来说，计算单个签名者的数量是不可能的。

在 3G 漫游中，情况有很大不同。当一个新的运营商产生时，其他的运营商不会自动想和这个新的运营商交换漫游流量，但是会和这个运营商达成一个合法协议并且建立一个技术隧道。在联邦 PKI 里，情况刚好相反：无需做任何事仍能够信任其他人。

在联邦 PKI 里, 文书工作和处理让证书中的命名约束变得毫无必要, IKE 想当然的不能和桥 CA 一起使用。

B.5 直接交叉认证方法的可行性

本章讨论直接交叉认证, 即手动交叉认证方法。在这种方法中, 只有在运营商同意和另一个运营商建立隧道时, 运营商才会做交叉认证。无论如何, 隧道建立是一个合法的技术性的操作, 因此此时做交叉认证也是可行的, 是撤销对桥 CA 交叉认证的初始步骤的需要。

关于直接交叉认证的可行性或者在 GRX 或者非 GRX 环境中上下文中的桥 CA, 没有技术上的不同。对于提供桥 CA 服务, GRX 可能是一种可能的选择。

B.5.1 直接交叉认证的好处

直接交叉认证的好处: 作为一种机制, 现有 PKI 产品相当了解且广泛支持这种机制, 并且如果这些产品开始充分支持这种机制, 甚至存在一条演进到一个桥 CA 解决方案的路径, 建立一个桥 CA, 运营商的数量就会变得足够大, 从而保证桥 CA 技术的使用。无论如何, 桥 CA 使用交叉认证机制。

隧道配置如下:

- Local-Subnetwork = some ipv6 subnetwork address;
- TrustedCA's = LocalCA。

允许哪一个运营商接入的信息在本地 CA 所作的直接交叉认证中是含蓄的, 因此认证和访问控制紧紧连接。如果不同的国外运营商需要接入不同的子网络, 每一个运营商会有单独的附有 SEG IP 地址的隧道配置, 包括一个“允许证书题目”限制。既然能被认证的运营商集只是那些在做直接交叉认证已经同意信任的运营商, 那么在这个模型 (和桥 CA 模型相比) 中“允许的证书签名者”限制并不是必需的。在桥 CA 的情形中, 能被认证的运营商集合包括所有已经和 bridge 连接的运营商。

B.5.2 内存和处理能力需求

如果是直接交叉认证, 每一个运营商应在本地存储颁发给其他运营商的证书。它们可以存储在 SEG 设备中, 或者尔后存储在公用的存储库中。

如果一个运营商和其他 500 个运营商达成漫游协议, 如果这个运营商自己签署证书, 而且一个证书需要 1kB 节内存, 可能总计需要大约 1000kB 内存。考虑到 SEG 硬件的高级末端特性, 应当是十分可行的。

证书生效的处理能力基准:

- 硬件: 800MHz 奔腾 III, 256MB 内存卡。
- 200x1024-bit RSA 证书, 1 个根 CA (运营商拥有的 CA), 200 个子 CAs (其他运营商的 CAs) 和 200 个网络设备 (SEG) 证书。CRLs 也需要检验。测试过程中, 要从磁盘上装载证书和 CRLs。整个测试大约 3.5s, I/O 磁盘可能占了大部分时间。

在这个测试中, 200 个证书链生效成为信任根源。

B.5.3 缺陷

就像上节分析的那样, 因为所有其他运营商的 SEG CA 证书不需要和其他运营商的存储在一起, 桥 CA 方法节省了 SEGs 中的内存或者存储空间。在 IKE 协商过程中, 只会存储桥 CA 证书, 并且找回其他证书。

B.5.4 至桥 CA 的可能演进路径

假如 PKI 产品的支持变为现实，如果需要的话，逐渐使用桥 CA 是有可能的。从一个运营商的角度来看，目前为止，桥 CA 会像任何其他的运营商，并且会做一个交叉认证。但是另外一方面，每次达成一个新的路由协议，就要更新给桥 CA 颁发的证书中的命名约束。

附录 C

(资料性附录)

SEGs 的 CRL 库接入协议

为了证明 SEGs 协议接入 CRL 库的决定, 本附录总结了两个候选技术的优缺点。

a) LDAP

——优点: 由所有 PKI 产品 (除非纯手动) 来执行。

——优点: 可测。

——优点: 灵活 (对其他系统的综合可能性, 自动找回公共密钥的可能性)。

——缺点: 复杂。

b) HTTP

——优点: 简单。

——缺点: 不是所有 PKI 产品都支持 (尽管受到广泛支持)。

选择 LDAP 作为更能经受未来考验的协议。尽管 LDAP 比 HTTP 复杂, 但在 PKI 的设备商和运营商中很好地建立了 LDAP。

附录 D

(资料性附录)

在 CR 中存储交叉证书的结论

为了证明在证书库中存储交叉证书，取出带有 LDAP 的交叉证书并且在 SEGs 中缓存的结论，本附录总结了三种选择中的优势和缺陷，见表 D.1。

表 D.1 三种选择的优缺点

问题	A) 交叉证书存储在SEGs中	B) 交叉证书存储在CRs中	C) 使用时，交叉证书存储于CRs中且缓存在SEGs
初始化问题：在交叉认证时存储交叉证书	交叉证书最初存储在几个位置，也就是说，存储在所有的SEGs（估计数量在2到10之间）中。 赞成点：- 反对点：证书最初应拷贝在几个地方。不同制造者的SEG可能会有其他O&M接口来处理证书	交叉证书最初存储在CR中。 赞成点：完全标准化的处理。证书最初只拷贝在一个位置。运营商无论如何都应有这个库（由于CRL处理）。 反对点：-	交叉证书最初存储在CR里。像B)那样的赞成与反对
使用问题：IKE阶段1期间的潜伏期	赞成点：没有额外的潜伏期 反对点：-	赞成点：- 反对点：额外LDAP质疑（交叉证书被质疑）产生更多的潜伏期。	赞成点&反对点：第一次就如在B)的情况，接下来几次就如在A)的情况
清理问题：删除证书 ^a	赞成点：- 反对点：应从几个位置删除交叉证书，也就是从所有的SEGs中删除	赞成点：只从一个单个的地方删除交叉证书 反对点：-	赞成点：- 反对点：应从CR和每一个SEG中删除交叉证书
安全问题	赞成点：不存在一个单独的失败点。 反对点：-	赞成点：- 反对点：CR描绘了一个单独的适合攻击者的失败点，例如，通过打断在CR上的通信，提交谢绝服务	赞成点：部分减轻了单个失败点 反对点：-
^a 这个功能只需要在下次CRL发表前撤销交叉证书			

分析：

- 在每个 IKE 阶段 1 协商里，选项 B) 需要一个额外的 LDAP 质询并且会介绍新的错误事例。
 - LDAP 潜伏期：缓存从 LDAP 到本地磁盘的信息，并且组装这些信息需要花费一段时间，不过实际上，这个时间是不重要的。
 - 相比选项 A)，选项 B) 和 C) 的优势是更容易管理，即只/从一个单独的地方存储和删除证书。
- 结论:选项 C) 是最可行的选择，因为它结合了选项 A) 和 B) 的优点。

附 录 E
(资料性附录)
TLS 协议的规格

注：本附录包括 3GPP TLS 规格。其他 3GPP 规范（例如 3GPP TS 33.203, 3GPP TS 33.220 等）参考本附录。因此本附录可能也应用于其他规范里说明的设备和网络节点。除了可能的例外，使用 TLS 的新规范都应参考这个规格。

TLS 终结点应遵循以下限制和扩展来支持 TLS:

- 不应该像 SSL3.0 过时那样来使用 SSL3.0。
- 至少应该支持 IETF RFC 4346 中所述的 TLS1.1。应该支持 IETF RFC 5246 中所述的 TLS1.2。
- 应该使用两个终点都支持的最高 TLS 版本。
- 应该遵循 IETF RFC 5246 中所述的 TLS1.2 给出的关于允许的和强制的加密组规则。另外，应该支持 IETF RFC 4346 中所述的 TLS1.1 的强制的加密组。不应使用有 CR4 的加密组。不应使用含有 NULL 完整性保护（或者 HASH）的加密组。
- 对于 TLS 压缩来说，应支持在 IETF RFC 5246 中 TLS1.2 说明的 CompressionMethod.null。选择性地支持在 IETF RFC 3749 中说明的其他压缩方法。
- 密钥交换方法不应该是匿名的。因此，不允许 IETF RFC 5246 中 TLS1.2 定义的以“TLS_DH_anon_WITH_”开始的加密组来保护一个连接。
- 如果 TLS 连接用以在 IETF RFC 2818 中所述的 TLS 上传输 HTTP，那么客户端不应建立连接“upgraded to TLS Within HTTP/1.1” 根据 IETF RFC 2817，而只应该在原始的 TCP 连接上建立隧道。

注：对于和 Release10 之前的网元的相互协作，允许退回到 IETF RFC 5246 中和 IETF RFC 4346 中描述的 TLS1.0 协议版本是必要的。

附录 F

(资料性附录)

TLS 证书手动处理

本附录的目的是，万一没有 TLS 证书的认证架构，为 TLS 证书处理提供可选的指导方针。

在这个附录中，会用到以下缩写： CA_A 是在 A 的网络中的认证授权； CA_B 是在 B 的网络中的认证授权； $Cert_A$ 是 A 的证书，并且 $Cert_B$ 是 B 的证书； I_A 是标识符集，A 可能用此标识符集辨认 B； T_B 是 B 信任的对等集。

F.1 TLS 证书登记

基于公共密钥技术和证书，可以实现在 TLS 中的相互认证。TLS 对等者 A 和 B 需要包括一个证书库，并且应该至少有一个认证授权 CA，这个 CA 能在 A 和 B 都属于的安全域内颁发证书。 $Cert_A$ 包括 A 的标识 I_A 集。每一个标识是充分资格域名 (FQDN) 的格式。类似的，B 的证书是 $Cert_B$ 。

在 B 的储备中的证书，定义了 B 信任的对等实体 T_B 群。有几个证书产生和注册的选项，其中三个描述如下：

1) 在一个选项中，只在 B 的网络中有一个认证授权 CA_B 。 CA_B 给 B 颁发一个证书 $Cert_B$ ，并给 A 颁发一个证书 $Cert_A$ 。这些证书以安全的方式“out of band”从 CA_B 递送给 A 和 B。然后 A 和 B 通过将对等证书插入证书中，把它们对等实体加入到它们信任的对等群中。这种插入是典型手动的，而且具体详情依赖于证书库备的管理接口的执行。

2) 在另一个选项中，A 和 B 的网络都各自包括认证授权， CA_B 和 CA_A 。 CA_B 给 B 颁发证书 CA_B ， CA_A 给 A 颁发一个证书。这些证书以安全的方式“out of band”从 CA_B 递送给 A 和 B。A 和 B 然后通过将对等证书插入证书储备，把它们对等实体加入到它们信任的对等群中：A 将 $Cert_B$ 插入到 A 的证书库中，B 将 $Cert_A$ 插入到 A 的证书库中。

3) 在第三个选项中，交换两边的 CA 证书：以一种安全的方式“out of band”，将 CA_B 的证书递送给 A， CA_A 的证书递送给 B，然后插入证书库中，标记为受信任的。 $Cert_A$ 和 $Cert_B$ 的有效性是基于证书库中相应 CA 证书的存在，在 TLS 握手时会相互交换 $Cert_A$ 和 $Cert_B$ 。

注：在选项 1 和 2 中，如果对等体自己产生签名证书并且以安全的方式“out of band”互换，有可能避免认证授权的需要。同样的，代替证书自己，在这些选项中，可能会以安全的方式“out of band”交换证书指纹。

F.2 TLS 证书撤销

在 PKI 撤销接口不在的情况下，证书撤销需要手动执行。撤销操作涉及 A 从 B 信任的对等体 T_B 群中删除。在以上描述的前两个登记选项中，撤销发生在 B 从证书库中删除 A 和 $Cert_A$ 的证书的时候。删除动作是手动完成的。在第三个选项中，A 和 $Cert_A$ 的证书不在 B 的证书库中。出于这个原因，B 应有一种方法来检查携带有证书颁发者的 $Cert_A$ 的合法性（同样的，在前两个登记选项中，如果 B 能检查携带有证书颁发者的 $Cert_A$ 的合法性，手动维护操作的数量会减少）。这个检查可以通过使用 IETF RFC 2560 中所述的在线证书身份协议(OCSP) 或者通过使用 IETF RFC 5280 中所述的 $Cert_A$ 颁发者发布的证书撤销列表(CRLs)来完成。

附录 G

(资料性附录)

初始登记的样本 CMPv2 信息流

本附录的目的在于提供一个基站初始登记可能如何执行的概览。

在图 G.1 中，显示了一个基站初始登记到 RA/CA 的信息流。信息流的预处理是基站包括设备商提供的公/私钥，而且提前提供相关设备商 CA 签名的基站证书。如果有一个证书链一直到设备商根 CA，同样的，中间这个证书应提供给基站。RA/CA 配置有设备商的根证书和它自己的证书。交换的信息是通过设置 PKIHeader 域的“protection”和“protectionAlg”来保护。

基站初始登记的信令流程如图 G.1 所示。

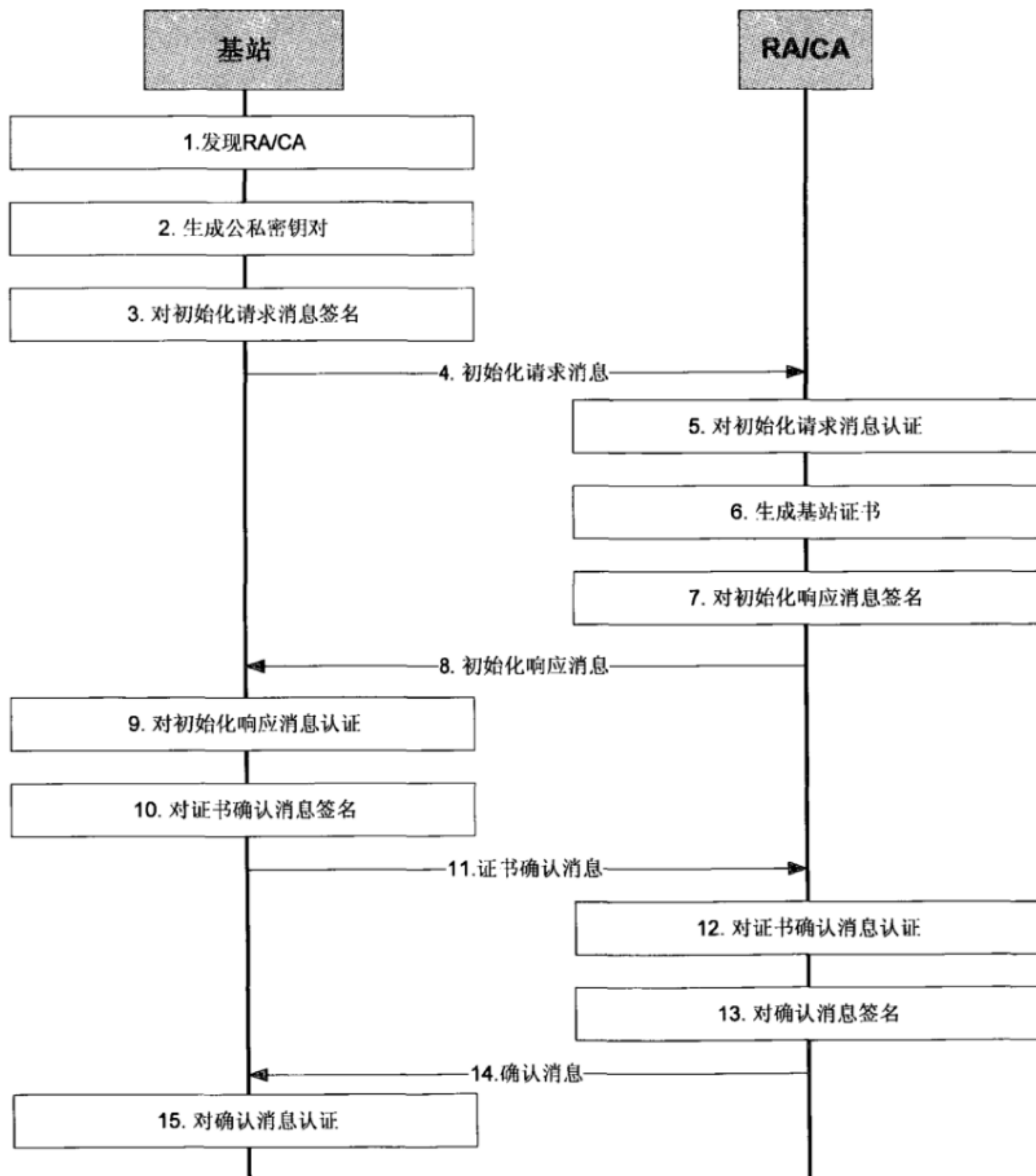


图 G.1 基站初始登记信息流程图

- 1) 基站发现 RA/CA 地址。
 - 2) 如果没有提前准备的话, 基站产生在运营商 CA 中登记的私钥/公钥对。
 - 3) 基站产生 Initialization Request (ir) 消息。在 ir 中的 CertReqMsg 说明了这个请求的证书。如果基站知道建议的身份, 它会将其包含在服从域。为了提供拥有证明, 基站使用 RA/CA 认证的与公钥有关的私钥为 CertReqMsg 的 POPOSigningKey 域产生签名。基站使用设备商提供的私钥签署证书, 并且将数字签名包含于 PKIMessage 中。它自己的设备商签名的证书和任一个中间证书包含在携带 ir 的 PKIMessage 的 extraCerts 域中。
 - 4) 基站将签名的 ir 信息发送给 RA/CA。
 - 5) RA/CA 检验 ir 信息上的数字签名, 以防设备上的根证书使用基站发送的证书。RA/CA 也验证请求证书的私钥的占有证明。
 - 6) RA/CA 为基站产生证书。如果建议的基站身份不包括在 ir 信息中, RA/CA 确定建议的基站身份, 例如, 基于生产商提供的基站身份, 此身份包含在基站证书中。
注: 运营商使用的基站身份的确定流程不在本标准范围内。根据 IETF RFC 4210, RA/CA 可能使用另一个基于本地信息的身份代替基站发送的建议的身份。
 - 7) RA/CA 产生一个包含颁发的证书的初始响应 (ip), 并且在初始请求中使用同样的 certReqId 值。RA/CA 使用 RA/CA 的私钥 (或者签署 CMP 信息的私钥, 如果单独的) 签署这个 ip, 并且在 PKIMessage 中包括签名, RA/CA 证书和运营商的根证书。认证 RA/CA 证书的合适的证书链也包含在 PKIMessage 中。
 - 8) RA/CA 将签署的 ip 发送给基站。
 - 9) 如果没有提前为基站准备运营商的根证书, 基站从 PKIMessage 中提取运营商的根证书。基站使用 RA/CA 证书来认证 PKIMessage, 并成功的安置基站证书。
 - 10) 基站生成并签署 CertificateConfirm (certconf) 消息。CertificateConfirm 消息在初始请求中使用同样的 certReqId 值。
 - 11) 基站将包含有签字的 CertificateConfirm 的 PKIMessage 发送给 RA/CA。
 - 12) RA/CA 认证包含有 CertificateConfirm 的 PKIMessage。
 - 13) RA/CA 生成并签署一个 Confirmation 消息 (pkiconf)。
 - 14) RA/CA 将包含有 pkiconf 的 PKIMessage 发送给基站。
 - 15) 基站认证 pkiconf 信息。
-

中华人民共和国
通信行业标准
移动通信网络域安全认证框架
YD/T 2909-2015

*

人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100164
北京康利胶印厂
版权所有 不得翻印

*

开本：880×1230 1/16 2015年12月第1版
印张：3.25 2015年12月北京第1次印刷
字数：84千字

15115·828

定价：35元

本书如有印装质量问题，请与本社联系 电话：(010)81055492