



中华人民共和国通信行业标准

YD/T 1972.2-2009

800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求 第 2 部分：用户数据类设备

Technical requirements for 800MHz/2GHz cdma2000 digital cellular
mobile telecommunication network multimedia domain equipment
Part 2: User data equipments

2009-12-11 发布

2010-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 缩略语	1
4 HSS 功能要求	2
4.1 功能逻辑	2
4.2 用户位置管理相关功能	3
4.3 鉴权功能	3
4.4 用户数据和业务数据管理	7
4.5 隐式注册	7
4.6 S-CSCF 分配	8
4.7 计费功能	8
5 性能及可靠性指标	9
6 接口要求	9
7 操作维护和网管要求	9
7.1 维护测试功能	9
7.2 故障检测及处理	9
7.3 状态监视及性能管理	10
7.4 系统实时控制	10
7.5 软、硬件更新	10
7.6 局数据修改	11
7.7 告警要求	11
8 定时与同步要求	11
9 电源及接地要求	11
10 环境要求	11

前 言

《800MHz/2GHz cdma2000数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》是根据我国CDMA网络的发展需要，参考3GPP2的系列规范，并根据我国国内的实际情况制定而成的。

YD/T 1972《800MHz/2GHz cdma2000数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》分为4部分。

- 第1部分：会话控制类设备；
- 第2部分：用户数据类设备；
- 第3部分：互通类设备；
- 第4部分：媒体资源类设备。

本部分是YD/T 1972的第2部分。

《800MHz/2GHz cdma2000数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》是“800MHz/2GHz cdma2000数字蜂窝移动通信网多媒体域（MMD）系统”系列标准之一，该系列标准的结构及名称如下。

- a) YD/T 1972《800MHz/2GHz cdma2000数字蜂窝移动通信网 多媒体域（MMD）系统设备技术要求》
 - 第1部分：会话控制类设备；
 - 第2部分：用户数据类设备；
 - 第3部分：互通类设备；
 - 第4部分：媒体资源类设备。
- b) YD/T 1973《800MHz/2GHz cdma2000数字蜂窝移动通信网 多媒体域（MMD）系统设备测试方法》
 - 第1部分：会话控制类设备；
 - 第2部分：用户数据类设备；
 - 第3部分：互通类设备；
 - 第4部分：媒体资源类设备。

本部分与 YD/T 1973.2《800MHz/2GHz cdma2000 数字蜂窝移动通信网 多媒体域（MMD）系统设备测试方法 第2部分：用户数据类设备》配套使用。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：工业和信息化部电信研究院、中国联合网络通信股份有限公司、中兴通讯股份有限公司。

本部分主要起草人：李侠宇、顾旻霞、王君珂、李振东。

800MHz/2GHz cdma2000 数字蜂窝移动通信网

多媒体域（MMD）系统设备技术要求

第2部分：用户数据类设备

1 范围

本部分规定了 800MHz/2GHz cdma2000 数字蜂窝移动通信网多媒体域的用户数据类设备 HSS 的功能要求、安全要求、操作维护及网管，性能及可靠性指标等内容。

本部分适用于 800MHz/2GHz cdma2000 数字蜂窝移动通信网中 MMD 系统的用户数据类设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YDN 065-1997	邮电部移动电话交换设备总技术规范书
IETF RFC 1305	网络时间协议（版本3）规范和执行
IETF RFC 2401	INTERNET协议安全结构
IETF RFC 3310	使用证明与密钥协议的HTTP摘要证明

3 缩略语

下列缩略语适用于本部分。

AAA	Authentication, Authorization, Accounting	认证、鉴权和计费
AC	Authentication Center	认证中心
AMF	Authentication Management Filed	认证管理域
AKA	Authentication and Key Agreement	认证和密钥协议
AS	Application Server	应用服务器
AUTH	Authentication Token	认证令牌
CAVE	Cellular Authentication voice Encryption	蜂窝鉴权与语音加密
CK	Ciphering Key	加密密钥
CSCF	Call Session Control Function	呼叫会话控制功能
ESP	Encapsulating Security Payload	封装安全负载
HLR	Home Location Register	归属位置寄存器
HSS	Home Subscriber Server	归属用户服务器
HTTP	Hyper Text Transfer Protocol	超文本传输协议
I-CSCF	Interrogating-CSCF	查询 CSCF
iFC	Initial Filter Criteria	初始过滤规则
IK	Integrity Key	完整性密钥

IKE	Internet Key Exchange	互联网密钥交换
IMS	IP Multimedia Core Network Subsystem	IP 多媒体网络子系统
IMSI	International Mobile Subscriber Identification Number	国际移动用户识别码
IP	Internet Protocol	互联网协议
MAA	Multimedia Authentication Answer	多媒体认证应答
MAR	Multimedia Authentication Request	多媒体认证请求
NTP	Network Time Protocol	网络时间协议
OSA	Open Services Architecture	开放业务体系
P-CSCF	Proxy-CSCF	代理 CSCF
PSI	Public Service Identity	公共业务标识
IMPU	IMS Public Identity	IMS 公有标识
IMPI	IMS Private Identity	IMS 私有标识
QoS	Quality of Service	服务质量
RAND	Random	随机
SA	Security Association	安全联盟
SHA	Secure Hash Algorithm	安全散列算法
SIP	Session Initiated Protocol	会话初始协议
S-CSCF	Serving-CSCF	服务 CSCF
UE	User Equipment	用户设备
URI	Uniform Resource Identifier	通用资源标志符
URL	Uniform Resource Locator	通用资源定位器
XRES	Expected Result	期望的认证应答

4 HSS 功能要求

4.1 功能逻辑

HSS 和其他关联网络实体间的逻辑如图 1 所示。

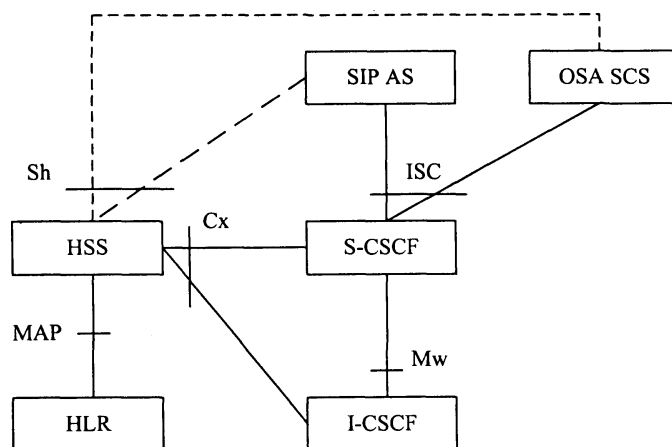


图1 HSS 和其他关联网络实体间的逻辑

4.2 用户位置管理相关功能

4.2.1 用户注册状态查询

HSS 应该支持 I-CSCF 通过 Cx 接口发起的用户注册状态查询,并根据查询要求返回正确的查询结果。

当收到 I-CSCF 通过 Cx 接口发起的用户注册状态查询时, HSS 应该检查该公共标识的 IMS 访问权限和相关的漫游协议许可情况,并通过 Cx 接口返回查询结果。

HSS 应该检查消息里面的公共标识和用户的私有标识是否相关。

当收到 I-CSCF 发起的查询时, HSS 应该能够提供用户的公共标识注册的 S-CSCF 地址或者 S-CSCF 地址列表。

当 HSS 检查到用户的公共标识未注册时,应该继续检查 I-CSCF 发出的查询请求中的 User-Authorization-Type 字段。如果 User-Authorization-Type 值为 DE_REGISTRATION,则 HSS 不返回任何 S-CSCF 名称或 S-CSCF 能力列表。如果 User-Authorization-Type 值为 REGISTRATION,则 HSS 需检查该用户是否存在有某个公共标识被分配有 S-CSCF。如果有则返回该 S-CSCF 名称,如果没有则返回 Server-Capabilities AVP。如果 HSS 没有返回任何 Server-Capabilities AVP,则 I-CSCF 可以自己选择适当的 S-CSCF。

4.2.2 用户位置查询

HSS 应支持 I-CSCF 通过 Cx 接口发起的位置查询请求,以获得给 IMPU 分配的 S-CSCF 名称。I-CSCF 发起该程序,每个 IMPU 执行一次。

HSS 在接收到 I-CSCF 发起的位置查询请求后,实现以下功能。

- a) 对注册的 IMPU 进行授权,检查 IMS 接入许可和漫游协议。
- b) 执行第一个安全性检查,确定消息中的 IMPU 和 IMPI 是否关联。
- c) 得到 IMPU 是 Registered 还是 Unregistered 的(即作为一个终止呼叫进行的注册或者有一个 S-CSCF 保存了用户的属性) S-CSCF 地址,或者 S-CSCF 要支持的能力集。
- d) 对于 UnRegistered 的 IMPU,检查 IMPU 是否签约了非注册业务,HSS 需要鉴彻 IMS 签约是否至少有一个 IMPU 分配了 S-CSCF 名称。如果没有给该 IMPU 分配 S-CSCF,HSS 可以返回所请求的 S-CSCF 能力信息,使得 I-CSCF 能够选择一个 S-CSCF。

4.2.3 S-CSCF 注册/注销通知

支持 S-CSCF 通过 Cx 接口发起的 S-CSCF 注册和注销请求,并根据请求返回正确的响应。

支持为用户的公共标识分配一个 S-CSCF,或者为一个或多个用户标识清除其关联的 S-CSCF 地址。

支持 S-CSCF 从 HSS 下载用户的相关信息。当 HSS 检查到请求消息中的 Server Assignment Type 为注册或重注册时,应相关的公共用户标识的注册状态为已注册。

4.2.4 HSS 发起的注销

HSS 可以通过 Cx 接口主动发起用户注销,告诉 S-CSCF 某个用户应该不再处于已注册状态。

HSS 可以同时为一个或多个用户公用标识发起注销请求。

4.3 鉴权功能

4.3.1 一般要求

鉴权包括 IMS 网络对用户和用户对 IMS 网络的双向鉴权过程,对于非法的网络,移动台会拒绝接入,提高了用户接入网络的安全性。S-CSCF 发起用户鉴权,索取鉴权参数,HSS 为 S-CSCF 返回正确用户鉴

权参数。

S-CSCF 可以通过 Cx 接口向 HSS 请求鉴权向量，通过 MAR 消息，携带 IMPU/IMPI。HSS 在收到 S-CSCF 的 MAR 请求后，准备鉴权向量，通过 MAA 消息发送给 S-CSCF。

HSS 可以通过注册或重注册过程在任何时候对客户进行认证。可以支持 IMS AKA、HTTP Digest、2G Cave-Based。

HSS 进行安全参数的计算要求见 IETF RFC 3310。

4.3.2 多种鉴权机制

HSS 应支持多种鉴权机制，包括：AKA 鉴权机制、HTTP Digest 鉴权机制、2G Cave-Based 鉴权机制。

4.3.2.1 AKA 鉴权

对于 AKA 鉴权机制，HSS 中存储的鉴权信息包括以下 4 种。

- a) IMPU/IMPI: IMS 用户公有标识、私有标识；
- b) K: 用户鉴权密钥；
- c) 鉴权算法：用于计算出鉴权向量；
- d) 认证管理域 (AMF)：作为鉴权算法的输入参数。

HSS 支持 SHA-1 或者 MD5 算法来产生并存储认证向量，HSS 一次可以产生多个认证向量，按照序列号排序。每一个认证向量包含以下部分：一个随机数 RAND、一个期望的响应 XRES、一个加密密钥 CK、一个完整性密钥 IK 和一个认证标识 AUTH。每一个认证向量对应一次 S-CSCF 与 IMS 用户的认证和密钥协商。

对于加密密钥 CK，采用 DES-EDG3-CBC，或 AES-CBC 算法。

对于完整性密钥 IK，采用 HMAC-MD5-96，或 HMAC-SHA-1-96 算法。

4.3.2.2 HTTP Digest 鉴权

HSS 支持 SIP Digest 来产生并存储认证向量，HSS 一次可以产生多个认证向量，按照序列号排序。每一个认证向量包含以下部分：一个 Digest Realm、一个 Digest Domain、一个 Digest Algorithm、一个 Digest QoP、一个 Digest H (A1)。每一个认证向量对应一次 S-CSCF 与 IMS 用户的认证和密钥协商。

其中，Algorithm 是用于产生鉴权参数的算法，缺省是 MD5。QoP (Quality of Protection) 为品质保证级别，当用于 IMS 鉴权时，QoP 的值需要设置为“auth”级别。H (A1) 为一个 Hash 值，其值通过 IMPI、Realm、password 计算出。

详细鉴权流程如图 2 所示。

其中：SM1~SM3 步骤类同于 IMS AKA 鉴权机制。

CM1: Cx-AV-Req (IMPI, m)。该步骤中，S-CSCF 需要判断使用 SIP Digest 鉴权机制，S-CSCF 向 HSS 请求 m 个 SIP Digest 鉴权向量 (SD-AV)。

CM2: Cx-AV-Req-Resp (IMPI, realm, domain, algorithm, qop, H (A1))。HSS 返回生成的鉴权向量。

SM4: 401 Auth_Challenge (IMPI, realm, nonce, qop, algorithm, domain)。S-CSCF 利用鉴权参数产生 nonce 值。

SM5~SM6: 401 Auth_Challenge (IMPI, realm, nonce, qop, algorithm, domain)。

SM7: REGISTER (IMPI, realm, nonce, response, cnonce, qop, nonce-count, algorithm, digest-uri)。UE 使用获得册参数计算 cnonce、response 等参数。

SM7~SM9: REGISTER (IMPI, realm, nonce, response, cnonce, qop, nonce-count, algorithm, digest-uri)。
S-CSCF 使用 UE 提供的参数 (cnonce、qop、nonce-count 等) 验证 response。

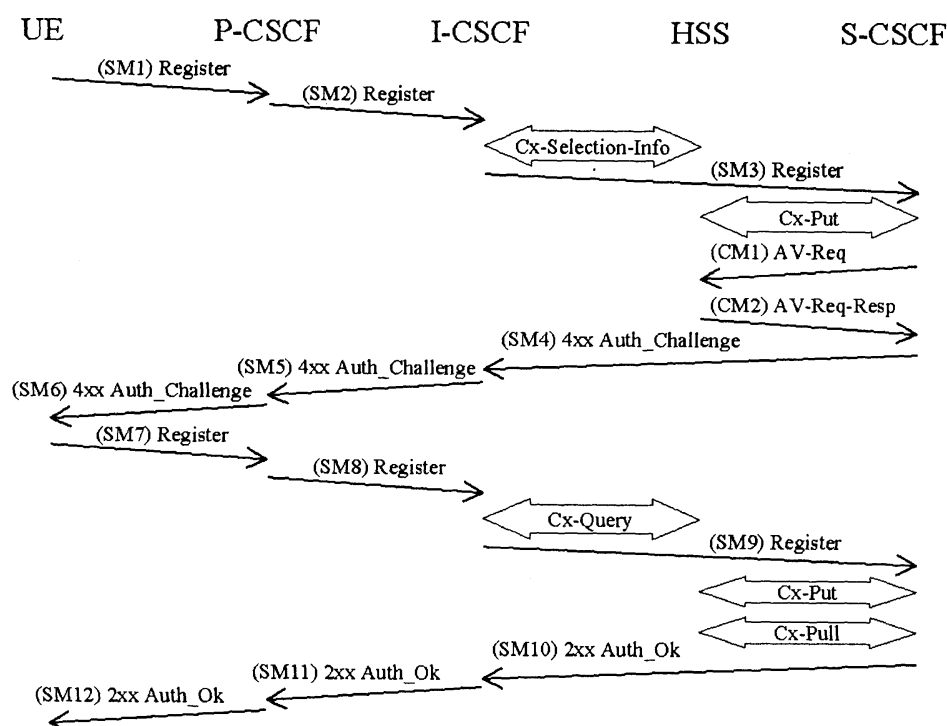


图2 鉴权流程

4.3.2.3 2G 卡 Cave-Based 鉴权

对于使用 2G R-UIM 卡的终端, HSS 应能支持 2G Cave-Based 鉴权功能。

对于 2G Cave-Based 鉴权机制, 在 HSS 中存储的鉴权信息包括以下 3 种。

- a) IMPU、IMPI: 用户公有、私有标识。
- b) 鉴权算法: 用于计算出鉴权向量。
- c) 鉴权管理域 (AMF): 作为鉴权算法的输入参数。

在 HLR/AC 中存储的信息有: IMSI: 国际移动用户标识符; A-key: 用于 Cave 鉴权机制的长期密钥。

当接收到 S-CSCF 的鉴权请求时, HSS 为该请求生成鉴权向量, 鉴权向量基于 AKA-AV 格式, 包括: 一个随机数 RAND、一个期望的响应 XRES、一个加密密钥 CK、一个完整性密钥 IK 和一个认证标识 AUTH。每一个认证向量对应一次 S-CSCF 与 IMS 用户的认证和密钥协商。

当使用 Cave-Based 的 AKA 鉴权机制时, HSS 根据 Cave 鉴权机制计算相关的参数, 添入 AKA AV 中, 提供给 S-CSCF。UE (ME) 使用 Cave-Based 算法验证参数并产生鉴权响应。

在 IMS 中使用基于 CAVE 的 AKA 鉴权机制的流程如图 3 所示。

步骤 1~6: 正常的 IMS 注册过程, 使用 AKA 鉴权机制, 但是 UE 所发起的注册请求中, Cave 相关的参数被封装成符合 AKA 鉴权机制的格式。

步骤 7~15: HSS 收到 S-CSCF 发送的鉴权请求后, HSS 根据用户配置判断 UE 不能支持完全的 IMS-AKA 鉴权机制, 即需要使用 Cave-Based 鉴权机制。HSS 从 IMPU、IMPI 分析出 IMSI, 并向 HLR/AC 发送 IS-41 AUTHREQ 请求, 并携带 IMSI。HSS 从 HLR/AC 中获取 CAVE Key, 并根据此计算 AKA_KEY。

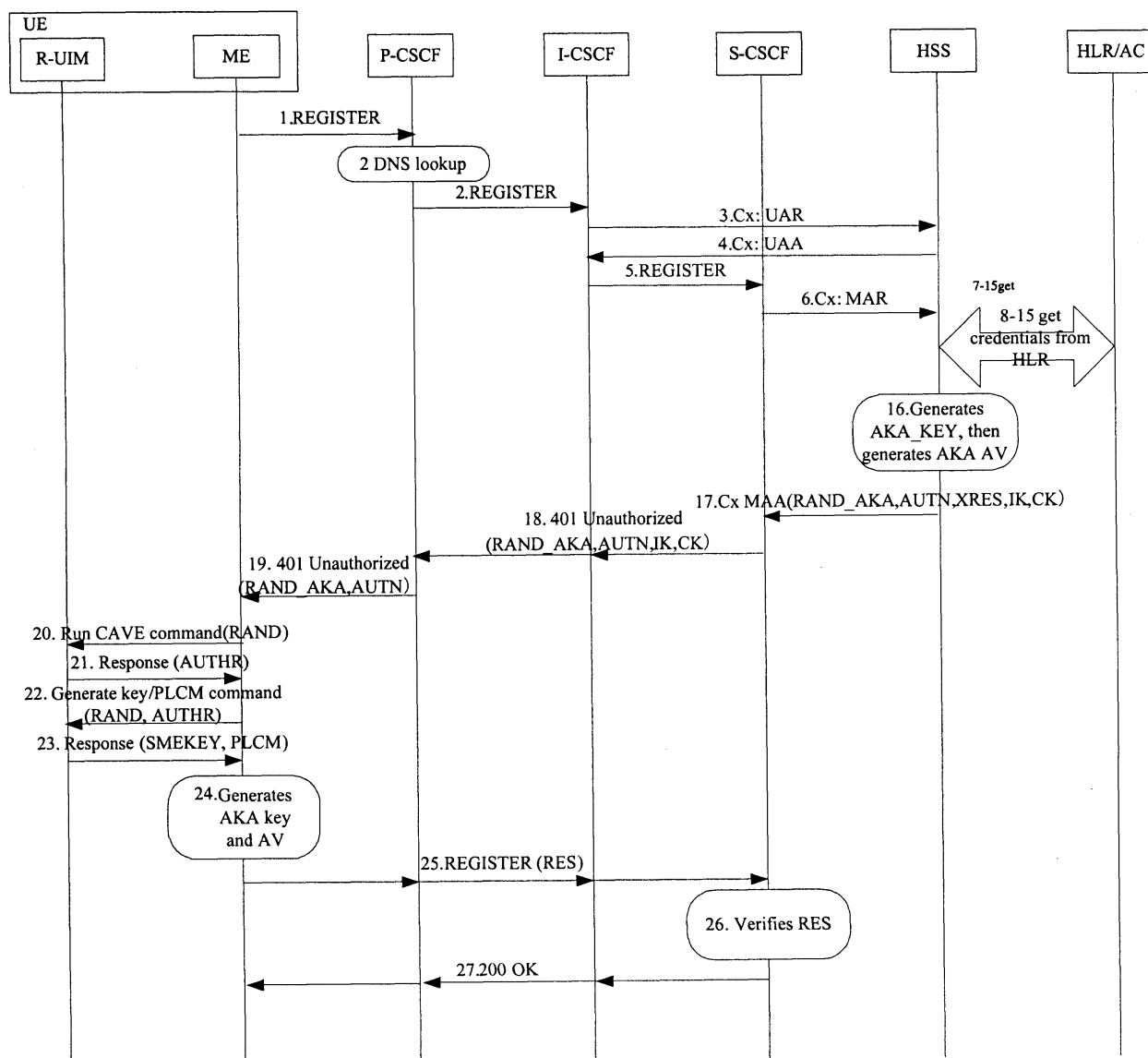


图3 基于 CAVE 的 AKA 鉴权机制的流程

步骤 16: HSS 计算 SQN_{HSS} 、 $RAND_N$ 、 $RAND_{M_{HSS}}$ ，使用 AKA_KEY 计算 MAC，并利用标准 AKA 算法计算出 $XRES$ 、 CK 、 IK 。HSS 按如下格式产生 AKA-AV: $AKA-AV = (RAND_AKA = RAND_N, AUTN, XRES, CK, IK)$ ，其中 $AUTN = (SQN_{HSS} \oplus AK \parallel AMF \parallel MAC)$ 。

步骤 17~19，正常的注册过程，鉴权向量被传递到 UE。

步骤 20，ME 接收到鉴权挑战后，从 $AUTN$ 、 $RAND$ 中提取 $RAND_M$ 、 $RAND_N$ 、 SQN ，ME 将由 $MIN2$ 、 $RAND_U$ 、 ESN 组成的 $RAND$ 发送给 R-UIM。

步骤 21: R-UIM 计算 AUTHR 响应。

步骤 22: ME 指示 R-UIM 产生 CAVE keys。

步骤 23: R-UIM 返回给 ME CAVE keys 和 SMEKEY。

步骤 24: ME 使用 R-UIM 返回的 CAVE keys，产生 $KEYSN$ 、 $KEYSM$ 。并且用以产生 $AKA_KEY = (KEYSM \parallel KEYSN)$ 。ME 同时计算 $XMAC$ ，并检测 $XMAC$ 是否等于 MAC 。另外，ME 也验证 $RAND_M$ 和 SQN 是否在合适的范围内。如果以上验证正确，则 ME 产生鉴权响应 RES。

步骤 25~27: 按照正常流程, 返回注册、鉴权响应。

4.3.3 网络域内的安全保护

HSS 可以支持以隧道模式的 IPsec ESP 对网络域内的信息进行安全保护, 可以支持 IKE 来产生 SA, 可以支持完整性保护, 数据源认证, 反重放保护以及可选的机密性的保护, 以上安全要求可以与安全网关结合使用 IPsec (见 IETF RFC2401) 来实现。

4.4 用户数据和业务数据管理

HSS 中应存储以下用户和业务信息。

- a) 用户身份标识: 包括私有用户标识和公共用户标识 (包括 SIP URI 和 TEL URL)。
 - b) 用户注册信息: 包括用户注册状态、用户当前所在的 S-CSCF 地址、S-CSCF Diameter 客户端地址、隐式注册公共用户标识组、S-CSCF 指派相关的信息 (用户需要的能力和默认 S-CSCF 的名称)。
 - c) 业务 profile: Initial Filter Criterion (包括 AS 地址和触发点)、PSI 信息 (I-CSCF 通过 HSS 查询时必须提供)。
 - d) 用户安全方面的信息: 存储并提供鉴权所需要的参数, 包括为支持 AKA、HTTP Digest、2G Cave-Based 等所需要的各种参数。
 - e) 计费信息: 包括主备用 CDF 和/或 OCF 的地址。
- iFC 中的业务信息是可选功能。支持共享的 iFC 是可选功能。

4.4.1 HSS 发起的用户数据更新

S-CSCF 的更新用户属性请求中只包含隐式注册集内的 IMPU 和相关的业务属性。

如果 IMPU 处于 Register 或者 Unregister 状态 (即作为一个终止呼叫进行的注册或者有一个 S-CSCF 保存了用户的属性), 并且用户属性有改变, 那 HSS 应立即把完整的用户属性传送到 S-CSCF 上。

当在 HSS 中修改了用户签约数据或者计费信息, 而这些数据同时存储在 S-CSCF。HSS 将完整的用户签约数据或者计费数据发送给 S-CSCF, HSS 采用推 (Push) 的方式下载用户签约数据给 S-CSCF。

4.4.2 S-CSCF 操作用户数据

如果 S-CSCF 发送 Server-Assignment-Request, 其中 Server-Assignment-Type AVP 的值为 USER_DEREGISTRATION_STORE_SERVER_NAME 或者 TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME, 并且 HSS 响应 DIAMETER_SUCCESS, 那在 IMPU 注销时 S-CSCF 应保存用户信息, 否则 S-CSCF 不应该保存。

S-CSCF 通过 Cx 接口和 HSS 进行用户数据交互。

当在 HSS 中修改了用户签约数据或者计费信息, 而这些数据同时存储在 S-CSCF。HSS 将完整的用户签约数据或者计费数据发送给 S-CSCF, HSS 采用推 (Push) 的方式下载用户签约数据给 S-CSCF。

4.4.3 SIP AS 操作业务数据

AS 通过 Sh 接口和 HSS 进行用户数据交互。

- a) HSS 应能支持 AS 发起 Sh-Pull 读取 HSS 中存储的业务数据;
- b) HSS 应能支持 AS 发起 Sh-Update 修改 HSS 中存储的业务数据;
- c) HSS 应能支持 AS 发起 Sh-Subs-Notify 订阅用户数据变更, 并在用户数据变更时通过 Sh-Notif 通知 AS。

4.5 隐式注册

HSS 应能支持用户公共标识的隐式注册。隐式注册功能支持用户在为某个公共标识注册的时候同时为一组相关的公共标识同时注册。

隐式注册分为 S-CSCF 发起的和 HSS 发起的两种方式。

a) S-CSCF 发起

当 S-CSCF 发起为一个用户公共标识注册的时候,该公共标识相关的隐式注册组里的所有公共标识即获得注册。

当 S-CSCF 发起为一个用户公共标识注销的时候,该公共标识相关的隐式注册组里的所有公共标识即获得注销。

当 S-CSCF 发起为一个用户私有标识注销的时候,该私有标识相关的隐式注册组里的所有公共标识即获得注销。

隐式注册组里的所有公共标识共享鉴权未决标志。

当 S-CSCF 从 HSS 下载用户公共标识签约数据的时候, HSS 需同时返回该公共标识所在的隐式注册组的用户相关数据。

b) HSS 发起

HSS 可通过主动发起到 S-CSCF 的更新来添加或者删除隐式注册组里的用户公共标识项。新添加的项目将共享组里的标识的注册状态。

HSS 不可以通过这种方式来删除隐式注册组里的最后一个用户公共标识。

HSS 可通过主动发起到 S-CSCF 的更新来对隐式注册组内的用户私有标识或某个用户公共标识进行注销。只要隐式注册组内的私有标识或某个公共标识被注销,则整个组的公共标识项被注销。

4.6 S-CSCF 分配

HSS 为 I-CSCF 提供可为用户提供服务的 S-CSCF 能力列表。I-CSCF 记录每个 S-CSCF 可提供的必选和可选能力,以便为用户选择合适的 S-CSCF。

4.7 计费功能

HSS (AAA) 应能支持离线计费功能。

对于 IMS, HSS (AAA) 的主要功能是,它提供了从 IMS 节点到网络运营商选择的营账系统的信息传递机制。主要功能有 3 项:

- a) 从 IMS 节点收集的会话计费信息的集合;
- b) 中间数据存储缓冲;
- c) 计费数据到营账系统的传递。

HSS (AAA) 作为近实时计费数据集合的存储缓冲。它将计费数据提供给营账系统。这些规格说明确定了 AAA 针对计费目的的外部接口,但是没有指定内部的功能性。然而, HSS (AAA) 的一些功能性被描述来指明它的行为。HSS (AAA) 可以执行特定的活动,如数据合并,数据域的预处理,过滤不需要的数据域,为指定的营账系统已定义的域添加运营商。这些操作能够优化转发给营账系统的计费信息,减少复载。

HSS (AAA) 能够以近实时模式从 IMS 节点接受数据。在文件模式下 (in file mode), 它有足够的存储来将收集到的计费数据传递给营账系统。HSS (AAA) 可以支持多个传输协议 (取决于营账系统所使用的)。HSS (AAA) 的目的之一是减少营账系统和 IMS 节点之间的发送计费数据的不同接口数量。如

果引入一个新的营账系统，它将被接口到 HSS (AAA)，IMS 节点的配置信息不需要修改。大容量媒介的使用和负载更加平均分布，因此 HSS (AAA) 可以被分布到多个物理节点来便于冗余。

5 性能及可靠性指标

HSS 的性能和可靠性参数包括以下 5 个：

- a) 用户最大容量 4000 万
- b) 支持的承载组网方式 SCTP
- c) 消息成功率 >99%
- d) 信息检索响应延时 95%概率<1000ms
- e) 用户登记延时 95%概率<2000ms

6 接口要求

HSS 应实现以下接口：

- a) 和 IMS 域的 CSCF 间的 Cx 接口；
- b) 和 IMS 域的 SIP-AS、OSA-SCS 间的 Sh 接口。

7 操作维护和网管要求

7.1 维护测试功能

HSS 设备的维护测试应能通过人机命令启动自动进行。

系统应具有对 HSS 中各种电路功能进行测试的测试系统，以便在维护中根据需要，随时或定期进行自动测试。在测试中通过的设备，应能在系统中正常投入使用，经一次或重复测试仍不能通过的设备或电路应自动闭塞或通过人机命令闭塞。

测试系统应包括专用的测试软件模块和必要的硬件测试电路。测试软件只有在需要时才有人机命令启动执行，并不影响系统的正常运行。在测试过程中，应能根据需要可用人机命令停止测试。

7.2 故障检测及处理

a) 一般要求

系统应备有自动诊断功能，应能检测软件、硬件的故障，对各种故障应具有记录的功能。硬件故障的检测应具有故障定位的功能，以便维护人员及时准确地处理故障。在发生硬件故障时，应能隔离有故障的硬件或自动倒换至无故障的备用硬件，保证系统继续正常运行。在发生软件故障时，系统应具有一定的自纠能力和自动恢复功能，其中包括再启动和再装入等。

当发生软件和硬件故障时，除应能打印输出故障记录报告外，对于重要故障还应发出可闻、可见信号，并应立即向本局操作维护中心送出报告。在无人值班时，本局的输出设备可以关闭，但相应的告警信号仍可送至操作维护中心。

b) 故障的容错性

当发生软件和硬件故障时，一般不应产生系统阻断。当发生的故障将不可避免地导致降低服务质量时，系统应能继续运行。系统中的重要设备可以具有备份或“n+x”的冗余。保证在发生故障时能自动脱离并进行倒换或进行系统再配置。

系统对某一硬件故障应经重复检测后进行确定，以防止偶发性故障造成系统的再配置或导致服务质

量的下降。

c) 硬件故障的定位

系统对硬件故障应具有自动诊断定位的能力。

d) 故障的恢复

当发生一般性软件和硬件故障时，系统应具有自愈能力，例如硬件发生故障时能立即倒换至无故障的电路继续正常运行，软件发生故障时能进行局部再装入等。当系统发生的全系统中断或电源中断恢复后，应能迅速地自动再启动运行。

1) 再启动

系统应提供不同等级的人工和自动再启动功能。系统再启动应具有记录，并打印输出相关资料。当系统产生自动再启动时，应有告警提示。

2) 再装入

系统应提供不同等级的人工和自动再装入功能。系统的再装入应有记录，并能打印输出相关资料。通过人机命令进行的不同等级的自动再装入，包括部分或全部软件、数据和参数的再装入。

e) 故障记录

系统应将所发生的各种故障进行及时记录，每月按故障种类输出故障统计表，也可以用人机命令索取前一天或前一周的故障记录。因故障而阻塞的电路数量超过预定值时也应作记录并送出警报。故障记录信息可在本局也可在操作维护中心输出。

7.3 状态监视及性能管理

本局或操作维护应可随时显示各种设备的状态信息和使用情况，并能记录统计信息，且通过人机命令接口查询。这些信息包括 HSS 之间的相关信令和统计信息。

7.4 系统实时控制

a) 设备闭塞

系统应能通过人机接口命令对接口链路和公共控制设备等进行闭塞和解闭等操作。某一设备被闭塞时，其上级公共控制设备应能与其断开。

b) 网络负荷超载控制

网络应有动态负荷超载控制能力及良好的拥塞解决方案，以确保网络在超载时维持最大的数据传输能力，在任何情况下不应由于异常数据流量造成全系统中断。

c) 业务实时控制

应能通过人机命令对某项业务的开放、停止、恢复等进行控制。

d) 网管控制

HSS 应能执行网管中心下达的网管控制命令。

7.5 软、硬件更新

系统设计应方便其软硬件的更新。

在更新过程中，应最大限度的降低中断业务的时间。所有更新的或修改过的软硬件应与原有的其他软硬件相兼容。

新软件引入之后，根据需要，旧软件应能被重新装入，并能够重新产生原有的局数据或其他数据。可以允许的数据丢失仅限于新软件引入至恢复旧软件期间产生的数据。

7.6 局数据修改

需要修改或补充的局数据，如路由、话费费率等，均能通过人机命令进行修改和补充。在修改和补充局数据时，应不影响系统的正常运行。

系统应能通过人机命令查阅局数据，也可传送到其他计算机上，进行脱机处理。

当需要大量输入数据时，系统应提供快速准确的输入手段。

局数据的查询和修改应能在本局也能在操作维护中心进行。

7.7 告警要求

a) 告警分类及告警信号

在 HSS 节点设备上可以记录历史告警，实时告警功能可以通过网管系统提供，另外也可以在人机命令行上提供实时告警功能。

1) 告警分类

HSS 局的告警应按照故障的严重程度进行分类，一般至少应分为两大类，即紧急告警和非紧急告警。

2) 告警信号

告警信号应为可闻和可视信号。可闻信号采用语音提示或声音提示，如果采用语音提示，直接报告告警级别，如果使用声音提示，不同声音表示不同级别。告警终端上提示信号显示。

b) 告警设备

配置系统时，需要指定一台告警终端。

c) 告警处理

告警信号可以被维护人员切断和停用，对无人值守的局告警指示应予停用。

在告警发生后，系统应能通过人机接口给出告警提示信息，并可根据维护人员要求进一步提供告警详细信息。例如，故障产生的起止时间，告警类别及故障的详细原因以及用于排除故障的文件手册名称、页号等。

8 定时与同步要求

HSS 等网元应具有与骨干网的网络时间同步的功能，可以通过 NTPv3（见 IETF RFC1305）协议等实现同步。

9 电源及接地要求

电源和接地要求见 YDN 065-1997。

10 环境要求

环境要求见 YDN 065-1997。

中 华 人 民 共 和 国
通 信 行 业 标 准

800MHz/2GHz cdma2000 数字蜂窝移动通信网
多媒体域（MMD）系统设备技术要求
第 2 部分：用户数据类设备

YD/T 1972.2-2009

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061

*

版权所有 不得翻印

*