

通信标准参考性技术文件

YDC 048-2007

电话号码映射（ENUM）总体技术要求

Overall Technical Specification for ENUM

2007-03-16 印发

中华人民共和国信息产业部科学技术司 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语定义和缩略语	1
3.1 术语定义	1
3.2 缩略语	3
4 提供ENUM功能的网络体系	3
5 编号要求	4
6 选路要求	4
6.1 PSTN	4
6.2 SIP系统	5
6.3 H.323 系统	5
6.4 多媒体消息系统	5
7 ENUM网关功能要求	5
7.1 E.164 号码到域名的转换功能	5
7.2 DNS查询功能	5
7.3 NAPTR资源记录	5
8 ENUM解析体系要求	8
8.1 ENUM全球解析体系的分层结构	8
8.2 解析体系的要求	8
9 注册管理要求	16
9.1 ENUM的提供模式	16
9.2 国家码的注册	17
9.3 用户号码的注册	18
10 协议要求	21
10.1 DNSSEC	22
10.2 HTTPS	22
10.3 EPP	22
10.4 TSIG	23
10.5 IXFR/AXFR	23
附录A （资料性附录） DNSSEC协议	24
A.1 概念	24
A.1.1 资源记录(RR, Resource Record)	24
A.1.2 资源记录集(RRset)	24
A.1.3 认证链(authentication chain)	24
A.1.4 信任起点 (Trust Anchor)	24
A.1.5 对密钥签名的密钥(KSK, key signing key)	25
A.1.6 区签名密钥(ZSK, Zone Signing Key)	25
A.1.7 消息验证码(MAC)	25

A.2 DNSSEC数据认证	25
A.2.1 DNSSEC中增加的资源记录.....	25
A.2.2 DNSSEC对服务器的要求.....	29
A.2.3 DNSSEC应答中RR的认证过程.....	29
附录B （资料性附录） TSIG和SIG（O）	33
B.1 TSIG	33
B.1.1 TSIG格式.....	33
B.1.2 TSIG计算.....	33
B.2 SIG(0)	34
B.2.1 SIG(0)资源记录.....	34
B.2.2 SIG(0)处理.....	34
附录C （资料性附录） 采用EPP协议提供和管理E.164 号码的技术要求	35
C.1 协议标识	36
C.2 对象标识	36
C.3 对象属性	36
C.3.1 域和主机名(Domain and Host Names)	36
C.3.2 联络和客户标识符(Contact and Client Identifiers).....	36
C.3.3 状态值(Status Values).....	36
C.3.4 日期与时间(Date and Time).....	37
C.3.5 有效期(Validity Periods).....	37
C.3.6 鉴权信息(Authentication Information).....	37
C.3.7 其他DNS资源记录属性.....	37
C.3.8 E.164 域名	37
C.3.9 NAPTR 字段(Field)	37
C.4 EPP业务连接的建立	37
C.5 E.164 相关EPP命令	38
C.5.1 通用EPP命令格式	38
C.5.2 E.164 号码相关EPP命令格式.....	38
C.6 EPP结果代码	43
附录D （资料性附录） 典型消息流程举例.....	46
D.1 PSTN用户呼叫SIP终端	46
D.2 SIP终端呼叫PSTN用户	47
D.3 多媒体消息业务	48

前 言

本标准文件的制定参考了 IETF 的 RFC 3761 “E.164 到 URI 动态授权发现系统 (DDDS) 应用 (ENUM)”、RFC 3401 “动态授权发现系统 (DDDS) 第一部分: DDDS 综述”、RFC 3402 “动态授权发现系统 (DDDS) 第二部分: 算法”、RFC 3403 “动态授权发现系统 (DDDS) 第三部分: DNS 数据库”、RFC 3404 “动态授权发现系统 (DDDS) 第四部分: URI 解析应用”、RFC 3405 “动态授权发现系统 (DDDS) 第五部分: URI.ARPA 分配程序”、RFC 1034 “域名—概念和设施”、RFC 1035 “域名—实施和规定”以及美国 ENUM 论坛“美国实施 ENUM 规范(#: 6000_1_0)”的基础。本标准文件中 Tier 1 系统和 Tier 2 系统的性能指标参考了“美国实施 ENUM 规范(#: 6000_1_0)”中的规定。

为满足要求,现将该标准文件印发,供科研、设计、生产、使用和管理等方面参照使用。使用中的建议和意见,请向起草单位或通信标准技术审查部反映。

本标准文件的附录 A、B、C、D 均为资料性附录。

本标准文件由中国通信标准化协会提出并归口。

本标准文件起草单位:信息产业部电信研究院、上海贝尔阿尔卡特股份有限公司、中兴通讯股份有限公司。

本标准文件主要起草人:张捷、张大坤、李成、张晓、洪钧。

电话号码映射（ENUM）总体技术要求

1 范围

本标准文件规定了在网络中提供ENUM功能的网络体系架构、编号要求、选路要求、ENUM网关的功能以及ENUM解析体系、注册管理和协议方面的要求。

本标准文件适用于指导ENUM功能在网络中的引入。

2 规范性引用文件

下列文件中的条款通过本标准文件的引用而成为本标准文件的条款。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文件，然而，鼓励根据本标准文件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文件。

RFC 2818 (HTTPS) TLS之上的HTTP (HTTP Over TLS) (2000.5)

RFC 2845 DNS 的密钥事务认证 (Secret Key Transaction Authentication for DNS (TSIG))

RFC 3730 可扩展提供协议 (Extensible Provisioning Protocol) (EPP)

RFC 3731 可扩展提供协议域名映射 (Extensible Provisioning Protocol (EPP) Domain Name Mapping)

RFC 4114 可扩展提供协议E.164号码映射 (E.164 Number Mapping for the Extensible Provisioning Protocol (EPP))

RFC 4033 DNS 安全引入和要求 (DNS Security Introduction and Requirements)

RFC 4034 DNS 安全扩展的资源记录 (Resource Records for the DNS Security Extensions)

RFC 4035 DNS安全扩展的协议更改 (Protocol Modifications for the DNS Security Extensions)

3 术语定义和缩略语

3.1 术语定义

下列术语和定义适用于本标准文件。

3.1.1

ENUM

ENUM的全称是电话号码映射，它定义了一套将电话号码映射为域名的规则，以及在DNS中存储与该域名相关联信息的方式。通过使用ENUM机制，一个电话号码对于主叫用户来说可以对应各种各样的地址，包括：电话、传真和电子邮件，即主叫用户可以通过一个电话号码给被叫用户打电话、发传真或发送电子邮件等；作为被叫用户，他/她可以规定适合于自己的通过单一号码接入的方式，即规定该单一电话号码所对应的电话号码、传真号码和电子邮件地址等，而且可以通过改变DNS中的相应的记录容易地更改他们的联络信息，不必改变接入的号码。

3.1.2

DNS

DNS是域名系统的简称，通过DNS系统，可以由一部机器的域名查其IP地址，也可以由机器的IP地址反查它的域名。

DNS由三个主要的组成部分：域名空间和资源记录、名字服务器以及解析器。层次树是组成DNS域名空间的基本组织形式，形式上看是一个倒置的树。

3.1.3

名字服务器

名字服务器是用来存储域信息的数据库。数据库被分成多个部分，每个部分称作“区”。如果一个名字服务器中加载了一个区的数据，则称这个名字服务器对整个区有权。通常，为了防止主机或者通信故障，多个名字服务器都可以对一个“区”有权。同样，一个名字服务器也可以对多个区有权。一个名字服务器可以分成以下三个部分：

- a) 数据库服务器：回答那些对于它有权的数据的查询
- b) 缓存：临时存储从其他名字服务器获得的数据信息
- c) 代理：帮助解析器完成查询

3.1.4

解析器

解析器是应用程序和域名服务器的接口。最简单的一种情况就是，解析器从应用程序接收到一个请求，同名字服务器交互后，将名字服务器返回的结果以本地用户程序可以识别的格式返回。应用程序通过名字解析器将一个主机名转换为一个IP地址，也可将一个IP地址转换为与之对应的主机名。解析器将向一个本地名字服务器发出查询请求，这个名字服务器可能会直接对查询返回结果，也可能通过某个根名字服务器或其他名字服务器来完成这个查询。

3.1.5

域名解析系统

域名解析系统是一个域名到地址的映射系统。域名解析采用客户端/服务器模式。客户端是解析器程序，它负责：查询域名服务器；解释从服务器传回的响应；将信息返回给请求方。服务器端为名字服务器，它存储有关域名空间的信息。域名解析有两种方式：

- a) 递归解析：由收到请求的名字服务器系统完成全部解析。
- b) 反复解析：每次联系一个不同的服务器。

每一个名字服务器都有可能收到一个只能由其它一些名字服务器来回答的查询，在这种情况下该服务器可以采用递归解析或反复解析的方式。如果采用递归解析的方式：由第一个服务器为客户端继续查询其他的服务器；如果采用重复解析方式，该服务器告诉客户端可以参考的其它的服务器。一般来说，客户端对本地DNS服务器都是递归查询，而DNS服务器之间的查询多是反复查询。

为了提高域名解析的效率，在解析系统中引入了缓存（Caching）技术。DNS服务器会把查到的结果（包括各种中间结果，如各级相应域的名字服务器的IP地址结果）暂存一段时间，这样当有其他机器发出相同的查询时，可以节省时间。

3.1.6

ENUM 网关

指支持ENUM功能的网络侧设备，包括将E.164号码根据相应的规则转换为符合规定的域名的功能、DNS查询功能以及能够正确的接收NAPTR资源记录的功能。

3.1.7

ENUM 服务器

ENUM服务器是指在ENUM解析体系中存储用户NAPTR记录的服务器。

3.1.8

注册管理机构（registry）

指维护授权的DNS注册表数据库的组织，负责主、从服务器并且为相应的域产生区文件。每个DNS区只能有一个注册管理机构。

3.1.9

注册服务机构（registrar）

直接向域名的注册人提供服务，为注册管理机构进行域名注册处理的组织。

3.1.10

注册人 (registrant)

指想要在DNS中注册域名的用户。注册的过程通常是通过注册服务机构进行的，注册完成后该注册人成为该域名的拥有者。

3.1.11

Tier 2 提供者 (Tier 2 provider)

Tier 2提供者负责提供Tier 2域名服务器，维护用户的NAPTR资源记录。

3.1.12

URI

URI为统一资源标识符，它包含URL和URN，定义了对任意命名和编址方式进行编码的语法。URL是统一资源定位符，是从因特网得到的资源位置和访问方法的简洁表示，格式为scheme://host:port/path，例如：<http://www.cnd.org/pub/hxwz>。URL中包含了过多的位置信息高效但却缺少灵活性，它最大的缺点是当信息资源的存放地点发生变化时，必须对URL作相应的改变。因此人们正在研究新的信息资源表示方法，例如：URN。URN为统一资源名，资源名字与位置无关。

3.2 缩略语

下列缩略语适用于本标准文件：

ASP	Application Service Provider	应用服务提供者
CNNP	Cross-network nameserver performance	跨网域名服务器性能
CSR	Customer Service Representative	客户服务代表
DDDS	Dynamic Delegation Discovery System	动态授权发现系统
DNS	Domain Name System	域名系统
DNSSEC	Domain Name System Security Extensions	DNS 安全性扩展
ENUM	Telephone Number Mapping	电话号码映射
EPP	Extensible Provisioning Protocol	可扩展提供协议
GUID	Global unique identifier	全球唯一标识符
HTTPS	Hypertext Transfer Protocol over TLS	TLS 上的超文本传送协议
IP	Internet Protocol	互联网协议
MAC	Message Authentication Code	消息认证码
NAPTR	Naming Authority Pointer	命名权威指针
PSTN	Public Switched Telephone Network	公共交换电话网
RR	Resource Record	资源记录
SIP	Session Initiation Protocol	会话发起协议
SRS	Shared Registration System	共享注册系统
TLS	Transport Layer Security	传送层安全
TSIG	Secret Key Transaction Authentication for DNS	DNS 的密钥事务认证
URI	Uniform Resource Identifier	统一资源标识符
URN	Uniform Resource Name	统一资源名
URL	Uniform Resource Locator	统一资源定位符
XML	Extensible Markup Language	可扩展标记语言

4 提供 ENUM 功能的网络体系

提供ENUM功能的网络体系如图1所示：

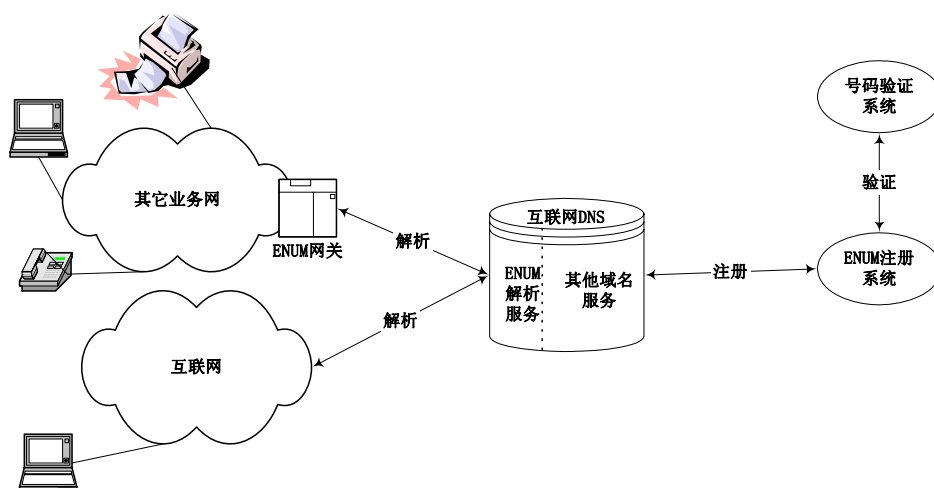


图1 提供 ENUM 功能的网络体系

为了提供ENUM功能需要在互联网域名解析体系中增加与电话号码相关的域名解析体系，该解析体系将完成电话号码域名到URI的映射。因此DNS解析体系在逻辑上包含ENUM解析服务和其他域名服务两部分。互联网以及电信网中的其它业务网都可以利用该域名解析体系获得存储于该体系中的与一个电话号码相关联的用户的各种通信联络信息，但在其它业务网中需设置支持ENUM功能的网关，该网关完成将E. 164号码根据相应的规则转换为符合规定的域名的功能、DNS查询功能、以及能够正确地接收NAPTR资源记录的功能。

为了提供ENUM功能还需要设置注册和验证系统。ENUM注册系统将接受注册人的注册申请，按照用户的要求将多种通信联络信息与用户的电话号码关联起来，并将相应数据放入ENUM解析体系中。在注册过程中，需要访问验证系统对注册申请者是否拥有相应的电话号码，以及该电话号码是否被停用等进行验证。

可以采用新建的方式设置ENUM网关，也可以采用将现有网络中相关设备软件升级的方式。

5 编号要求

如果网络已经具备了根据用户的属性或数据区分用户是否注册了ENUM应用的能力，用户可以直接申请将已经拥有的E. 164号码注册到ENUM解析系统中以提供ENUM应用，此时不需要给用户分配额外的号码。如果网络不具备该条件，为了便于选路，需要为ENUM应用分配特殊的号码段。号码的结构为：

$$1XY+X_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$$

其中：

1XY—ENUM应用标识码；

$X_1X_2X_3X_4$ —号码组标识，由相关主管部门分配。根据业务需求，可以为一个应用提供商分配一个或多个号码组；

$X_5X_6X_7X_8X_9X_{10}$ —用户号码，由应用提供商自己分配。

ENUM应用号码是作为一种业务号码来分配的，可以分配给申请使用基于ENUM的各种应用的用户，该号码不与具体的终端绑定。

该号码可以在国际呼叫中作为被叫号码的一部分，即作为被叫号码时可为： $86+1XY+X_1X_2X_3X_4+X_5X_6X_7X_8X_9X_{10}$ ，至于对方国家采用的具体的用户拨号方式视网络情况而定。

6 选路要求

6.1 PSTN

交换机在收到 $1XYX_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$ 后，根据 $1XY$ 判别出该呼叫涉及ENUM应用，应将呼叫接续到最近的ENUM网关，由ENUM网关查询DNS系统ENUM服务器后，根据所获得的信息完成呼叫的接续。

6.2 SIP 系统

SIP客户端或SIP服务器收到 $1XYX_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$ 后，按照ENUM应用进行处理。

6.3 H. 323 系统

H. 323网守收到 $1XYX_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$ 后，按照ENUM应用进行处理。

6.4 多媒体消息系统

MMS Relay/Server收到 $1XYX_1X_2X_3X_4X_5X_6X_7X_8X_9X_{10}$ 后，按照ENUM应用处理。

7 ENUM 网关功能要求

ENUM网关需要支持的功能包括：将E. 164号码根据相应的规则转换为符合规定的域名的功能，DNS查询功能，能够正确的接收NAPTR资源记录的功能。

7.1 E. 164 号码到域名的转换功能

假设e164. arpa将用于提供存储E. 164号码的DNS框架。将一个规定的E. 164号码映射为一个域名，需要遵循以下步骤：

- 将E. 164号码写成完整的格式，要包含国家码，如：+86-1XY-1234567890；
- 将所有的非数字的字符去掉，“+”号除外，如：+861XY1234567890；
- 将数字以外的所有字符去掉，如：861XY1234567890；
- 在每个数字之间加上“.”，如：8.6.1.X.Y.1.2.3.4.5.6.7.8.9.0；
- 将数字的顺序颠倒一下，如：0.9.8.7.6.5.4.3.2.1.Y.X.1.6.8；
- 将“.e164. arpa”加到字符串的尾部，如：0.9.8.7.6.5.4.3.2.1.Y.X.1.6.8.e164. arpa。

因此E. 164号码86-1XY-1234567890所对应的域名为：0.9.8.7.6.5.4.3.2.1.Y.X.1.6.8.e164. arpa。

7.2 DNS 查询功能

ENUM网关应支持解析器的功能，即查询域名服务器，接收从服务器传回的响应，将信息返回给请求方。与域名服务器之间支持DNSSec协议或者其他安全性协议（如基于IPSEC的DNS协议）。

7.3 NAPTR 资源记录

在ENUM解体系系统中，与电话号码相关联的信息是以NAPTR资源记录的形式存储的。NAPTR资源记录是DDDS系统数据库中用于存储规则的一种资源记录。DDDS称为动态授权发现系统，它用于实现字符串到数据的松散绑定，以支持动态配置的授权系统。DDDS是通过反复应用字符串转换规则直到达到结束条件，从而将一些唯一的字符串映射成为存储于DDDS数据库中的数据来实现其功能的。DDDS算法是基于改写规则的概念，这些规则被收集到一个DDDS规则数据库中，并可以通过给定的特殊的关键字接入。当将一个给定的规则应用于一个应用唯一串（Application Unique String）时，会将该串转换为一个新的关键字，该关键字可用于从规则数据库中再检索新的规则，所得到的新的规则然后可以再应用于原来的应用唯一串，这样循环往复，直到遇到结束条件。不能够对前一个规则的输出结果应用规则，所有改写规则必须总是应用于同一个算法开始时的应用唯一串。

如果用一个图表来表示DDDS算法，则如图2所示，ENUM只是DDDS的一个应用。

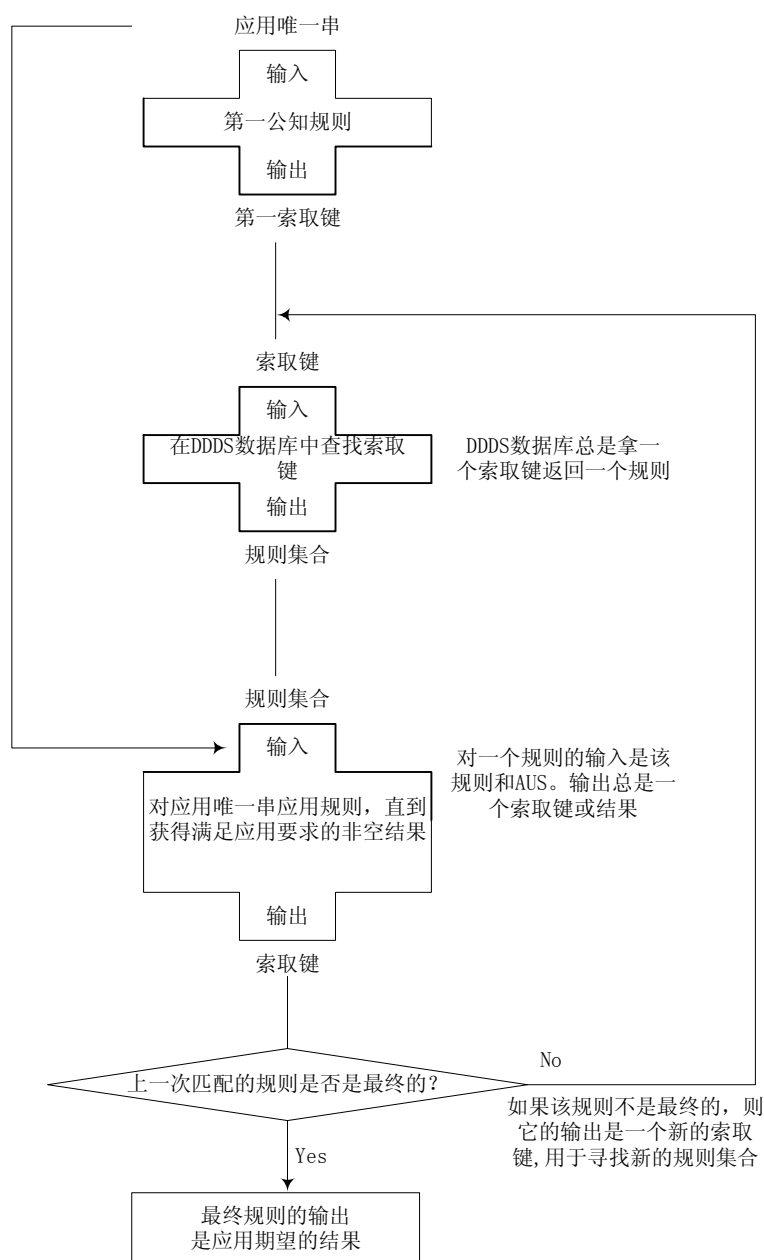


图2 DDS 算法

在 ENUM 应用中，应用唯一串是除去了非数字字符（但不包括数字最前面的“+”）的 E.164 号码。例如 E.164 号码“+86-1XY-1234567890”，将“+”以外的所有非数字字符都去掉，成为“+861XY1234567890”，就是应用唯一串。第一公知规则(First Well Known Rule)是同一规则，该规则的输入和输出是相同的。例如如果输入是“+861XY1234567890”，应用第一公知规则产生同样的字串“+861XY1234567890”作为输出。为了将这个输出转换为数据库的唯一索取键(KEY)，该字串需要根据 7.1 节中描述的规则转换为一个域名，用这个域名来请求 NAPTR 记录，该记录可能包含最终结果。如果“标志”为空的话，也可能产生一个从 DNS 返回的域名形式的新的索取键。目前 ENUM 应用中只定义了一个标志“U”，该标志意味着这个规则是最后一个，该规则的输出就是一个 URI。在 DDS 的 ENUM 应用中最后一次 DDS 循环的输出是 URI。目前 ENUM 应用只规定了一个 DDS 数据库。在 DDS 数据库中是利用 NAPTR 资源记录来包含改写(rewrite)规则的。数据库的索取键被编码为域名。

NAPTR (Naming Authority Pointer) 资源记录的格式如图3所示：

ORDER
PREFERENCE
FLAGS
SERVICES
REGEXP
REPLACEMENT

图3 NAPTR 资源记录的格式

该资源记录中各字段的含义如下：

次序(order)：该字段是一个 16 比特的无符号整数，用于指定对 NAPTR 资源记录处理的顺序；

优选项(preference)：这是一个 16 比特的无符号整数，它规定了对具有相同“次序”值的 NAPTR 资源记录的处理顺序，较低的值在较高值之前处理；

标志(flags)：该字段用于控制在 NAPTR 资源记录中对一些字段的重写和解释特征。目前 ENUM 应用中只定义了一个标志“U”，该标志意味着这个规则是最后一个，该规则的输出就是一个 URI。

业务(services)：该字段用于规定应用于该授权路径的业务参数。在 ENUM 应用中，该字段的值形式如下：

```
service_field = "E2U" 1*(servicespec)
servicespec   = "+"enumservice
enumservice   =type 0*(subtypespec)
subtypespec   =":" subtype
type           = 1*32 (ALPHA / DIGIT)
subtype       = 1*32 (ALPHA / DIGIT)
```

——即：一个必选的"E2U"（用于指示记录中为仅适用于ENUM的改写规则）后面跟着一个或多个 Enumservice，指示一个给定端点所提供的功能类别。每个Enumservice由一个初始的'+'字符指示。

——一个enumservice必须通过RFC的描述到IANA注册。对Enumservices的规定包括功能的规定（即它可以用来做什么），有效协议，和可能返回的URI方案。Enumservice的“type”或“subtype”字符串在语法上与URI方案或协议没有隐含的映射关系，如果他们之间存在某种映射关系，则必须要在该Enumservice的规定中说明。对于一个具体“type”的注册中必须规定允许哪些“subtype”。

——“type”和“subtype”注册规则的唯一例外就是用于实验目的情况，他们是以“X-”开头的。这些是未注册的，实验性的，并且只能在双方都同意的情况下才可以使用。

REGEXP：该字段是一个包含置换表达式的字符串，该表达式将被应用于客户端所持有的初始字符串以组成下一个要查找的域名。

替换(replacement)：根据“标志”字段的取值，该字段为要查询的下一个域名。当 REGEXP 是一个简单的替换操作时使用该字段。该字段和 REGEXP 字段一起组成了 DDDS 算法的置换表达式。

下面是一个 NAPTR 记录的例子。

下面举个例子，说明 ENUM 应用中可能返回的 NAPTR 记录的格式，本例中，我们可能获得下列的 NAPTR 资源记录(包含在消息的应答字段中)：

```
$ORIGIN 4.3.2.1.6.7.9.8.6.8.e164.tld.
IN NAPTR 10 100 "u" "E2U+sip" "!^.*$!sip:info@example.com!".
IN NAPTR 10 101 "u" "E2U+h323" "!^.*$!h323:info@example.com!".
```

IN NAPTR 10 102 "u" "E2U+msg:mailto" "!^.*\$!mailto:info@example.com!".

在本例中，域名4.3.2.1.6.7.9.8.6.8.e164.tld最希望使用SIP，其次是通过H.323语音，最后是通过SMTP消息方式。无论是用哪种方式，下一步解析需要使用各协议（SIP、H.323以及mailto URI规定）的解析机制来确定需要与网络中的哪一点联络。

8 ENUM 解析体系要求

DNS系统中需要建立相应的解析体系对由E. 164号码转换的域名进行解析，该解析体系将是一个全球解析体系，它的根是互联网DNS的根，该解析体系将为全球的ENUM应用提供解析服务。我国ENUM解析体系将是该解析体系的一部分。

8.1 ENUM 全球解析体系的分层结构

ENUM的全球解析体系如图4所示：

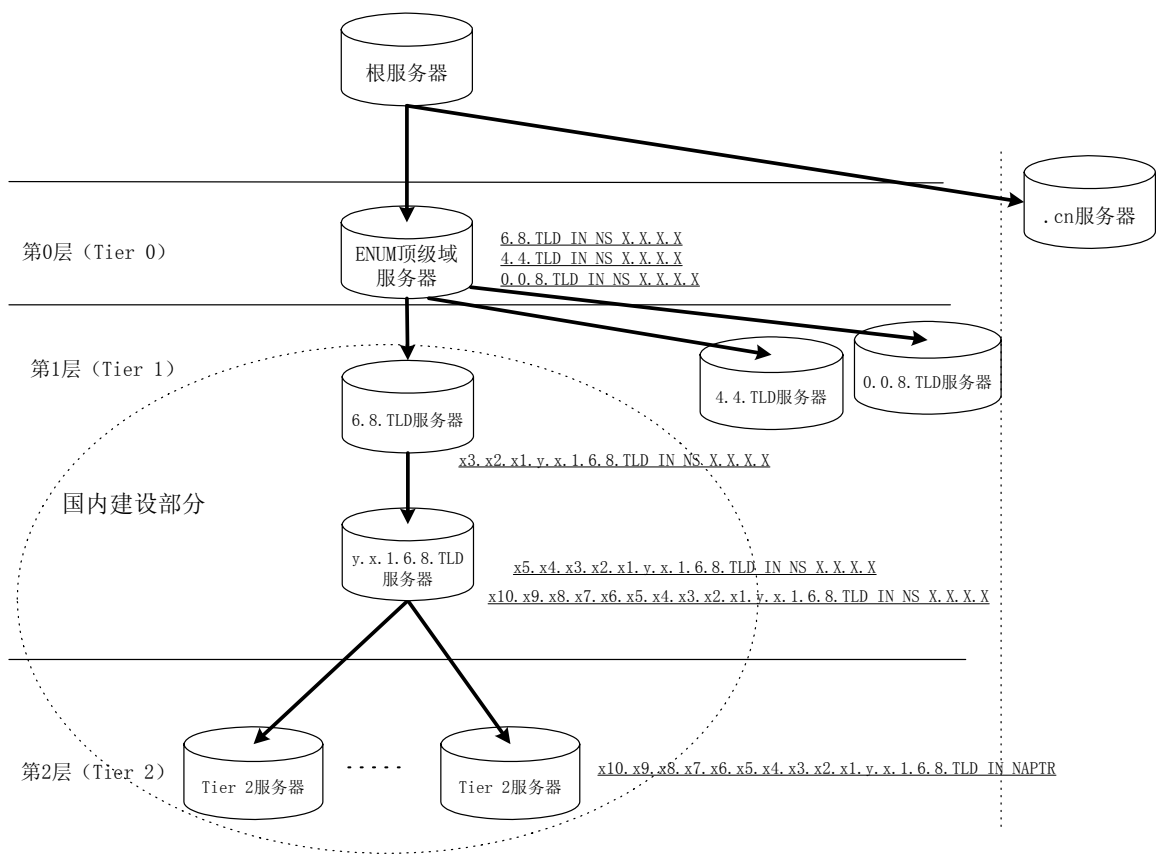


图4 ENUM 全球解析体系分层结构

ENUM解析体系在逻辑上分为三层，如图4所示，其中Tier 0是由国外组织管理的，对应于Tier 0的服务器分布于多个国家，其中有一台服务器设置在中国。第0层的域名服务器中包含的记录指向ENUM第1层的域名服务器。

对应于Tier 1和Tier 2层的服务器是由国内建设和管理的，Tier 1用于存放与E. 164号码相关的DNS记录，在该域的域名服务器中包含的记录指向一个完整的E. 164号码、一个E. 164号码段，或者是E. 164号码的一部分。在物理上Tier 1可由两级服务器组成，包括6.8. TLD服务器和y. x. 1. 6. 8. TLD服务器，6.8. TLD服务器中包含的记录指向一个1XYX₁X₂X₃号段，y. x. 1. 6. 8. TLD服务器中的记录指向一个完整的E. 164号码、一个E. 164号码段，或者是E. 164号码的一部分。

Tier 2用于存放注册到ENUM系统中的E. 164号码对应的NAPTR记录。

8.2 解析体系的要求

8.2.1 Tier1 系统的要求

Tier 1系统的主要功能是负责存储管理ENUM域名的NS记录,对相应的DNS查询作出响应。

8.2.1.1 共享注册系统 (SRS)

一个Tier 1注册管理机构被看作是共享注册系统,各注册服务机构可通过共享注册系统将他们客户的ENUM域名注册到我国的ENUM域名空间中。

Tier 1共享注册系统应满足以下要求:

- a) 允许多个授权的注册服务机构将ENUM域名注册到我国的ENUM域名空间中,且对注册服务机构的数量没有限制。
- b) 对所有的注册服务机构提供平等的接入完成与注册相关的操作,例如:
 - 1) 注册新的ENUM域名、联络信息或主机名;
 - 2) 检查已注册的ENUM域名、联络信息或主机名的状态;
 - 3) 删除已注册的ENUM域名、联络信息或主机名;
 - 4) 恢复已注册的ENUM域名、联络信息或主机名;
 - 5) 更新与已注册的ENUM域名、联络信息或主机名相关的信息;
 - 6) 在互相竞争的授权的注册服务机构之间转移ENUM域名注册。
- c) 在注册管理机构和授权的注册服务机构之间支持开放协议接口,即IETF定义的可扩展提供协议(EPP)以及相应的扩展。
- d) 与ENUM域名注册相关的联络信息(注册人、管理的、技术的等)存储于SRS之中。
- e) 拒绝来自ENUM注册服务机构的非法命令和请求(例如:丢失了必备数据元素)。
- f) 检出对同一ENUM域名的双重注册,并且通知提出请求的ENUM注册服务机构。在必要时,在争议期间Tier 1注册管理机构必须采取适当的措施保护被分配电话号码一方的权益。
- g) 支持批量文件处理。
- h) 根据规定的程序更新“区文件”(zone file)。

8.2.1.2 注册管理机构数据库

ENUM Tier 1注册管理机构将所有与ENUM域名注册相关的对象存储于注册管理机构数据库中。与Tier 1注册相关的对象主要有三个,它们是:域、主机和联络信息。注册管理机构的数据库应该以快速响应、可升级、支持并发处理方式运行。

注册管理机构的数据库应满足以下要求:

- a) 应允许来自多个注册服务机构的并发操作。
- b) 应根据EPP协议集的规定,支持注册服务机构对注册管理机构对象的操作,例如生成、查询、更新、删除和转移。
- c) 注册管理机构的数据库及其数据备份应该位于地理上分散的数据中心,以获得高可用性,并且实现数据的备份和恢复。

8.2.1.3 区文件

一个区文件包含DNS正确完成相应功能所需要的技术信息,即它包含了一个域中除了分配出去让其它组织管理的子域以外的域名数据信息。在传统意义上来讲,区文件的产生是指从注册管理机构数据库产生区信息,将它配置到主服务器,然后将其传播到辅服务器。后面这两步也称为区文件或区数据的传播。

Tier 1 注册管理机构对区文件的操作应满足以下要求:

- a) SRS应提供从注册管理机构数据库周期性生成区文件的方式,以便及时地反映通过注册管理机构-注册服务机构之间的接口完成的变更。
- b) 区文件一旦由SRS产生,就应该在最小时延内被可靠和安全地传播到所有的ENUM Tier 1域名服务器。
- c) 区文件的产生和传播程序不应应对正常的注册管理机构和域名服务器操作产生负面影响。

- d) 注册管理机构应该向注册服务机构提供能够通过自动方式更改他所负责的ENUM域名的接口。
- e) ENUM Tier 1注册管理机构的各域名服务器应该被放置于地理上分散的数据中心，以允许最大程度的冗余，抵抗灾难和故障。
- f) SRS应对所有的区文件更新支持日志记录和备份的能力。

8.2.1.4 联络信息

在ENUM中不使用传统的WHOIS业务，而采用一种称为ContactInfo的第三方诊断业务，该业务提供了一种不危及ENUM注册人隐私的联络必要实体解决问题的方式。当被问及ENUM域名时，Tier 1注册管理机构应返回为该域名提供服务的注册服务机构的联络信息，而不是注册人的联络信息。如果据此信息联络到注册服务机构，再由注册服务机构联络注册人，并且将问题报告转交给注册人或他们指定的联系人。注册服务机构一般情况下不提供注册人的联络信息，除非注册人有欺骗或违法行为时，才会将他们的联络信息透露给相关机构。注册管理机构应该依照相关的隐私政策接入“ContactInfo”数据检索。

8.2.1.5 统计报告

ENUM Tier 1注册管理机构应提供统计报告服务，并允许ENUM注册服务机构为它们的客户检索报告。一个注册管理机构应为每一个ENUM注册服务机构生成以下报告：

- a) 从帐务处理日志生成对帐报告日报；
- b) 注册服务机构域名注册累计报告日报和月报；
- c) 事务处理日志；
- d) 所拥有的所有数据完整的信息的输出文件。

注册服务机构累计报告应包括以下内容：

- a) 所处理的ENUM域名总数；
- b) “已注册”的ENUM域名总数；
- c) “不可用”的ENUM域名总数；
- d) “无效”的ENUM域名总数。

注册管理机构可提供客户报告服务，注册服务机构可规定报告的准则并且在报告完成后可以通过下载获得报告，该报告可以包含以下内容：

- a) 在任意时间段内注册的域名的数量和名称；
- b) 在一个规定的时间段内转移到注册服务机构或从注册服务机构移出的域名；
- c) 所有权变更的动作以及请求被处理的时间/日期。

这些报告应该被放置在安全的站点上，各注册服务机构可通过输入用户名和密码接入该站点。只有发起的（sponsored）注册服务机构被授权可以接入它的客户记录的报告。报告的格式应便于注册服务机构通过机器读取（例如XML，CSV）。报告名称应标识注册服务机构、报告生成的日期并指示报告的主题。注册管理机构应对所有生成的报告存档。

8.2.1.6 数据库备份

为了防止由于故障等原因导致数据的丢失，应对注册管理机构的数据提供备份。为了防止在火灾、洪水、或其他自然或人为灾害中丢失所有的设施，应对注册管理机构的数据提供异地容灾机制。

Tier 1注册管理机构应该对以下内容作出规定：

- a) 数据备份的频率和程序；
- b) 数据备份使用的硬件和软件系统；
- c) 恢复数据和重建数据库的程序。

此外还要求Tier 1注册管理机构提供以下的保护措施：

- a) 数据备份和异地容灾机制不应妨碍注册管理机构正常操作的整体性能；
- b) 数据备份和恢复程序应将注册管理机构的数据丢失和业务中断降低为最小。

8.2.1.7 网络操作和维护

ENUM系统需要提供完全并发的和高可用的服务,因此需要对Tier 1注册管理机构的各个方面进行操作和维护,以将其保持在较高的业务水平,主要包括对系统运行中断的预防、系统恢复程序以及技术支持等。

8.2.1.7.1 系统运行中断预防

Tier 1注册管理机构应具有专门设计的运行中断预防措施,以减少系统宕机时间。宕机时间可能是计划外的,由于外部电信、电源、国际网络或计算机设备的故障所致;也可能是计划内的,由于例行维护导致系统不可用时发生(例如:在软件或硬件升级和系统备份期间)。

Tier 1注册管理机构应该做到:

- a) 使用冗余和高可用系统体系结构以消除整个系统计划内的宕机时间,即当系统的一部分正在进行软件或硬件的升级以及系统备份时,注册服务仍然是可操作的;
- b) 使用冗余和高可用系统体系结构以减少计划外的宕机时间;
- c) 使用综合的系统监视程序在体系的多个层次上检出和解决问题,包括处理器、内存、操作系统、数据库、应用处理和网络连接;
- d) 实施严格、具体的保证措施,控制对所有数据中心设施的接入,防止对注册管理机构设施未授权的物理接入;
- e) 加强对所有注册管理机构子系统的技术安全措施,它们应该是严格的多层次的,防止对注册管理机构系统的未授权的电子接入。这些措施应该覆盖对各种数据库的接入控制以及网络和传输层的安全性和对非法进入的检出;
- f) 在所有数据中心都有备份软件、操作系统和硬件可用;
- g) 尽量使用最新的技术支持处理程序,以确保相应的人员能及时地解决所有的问题。

8.2.1.7.2 系统恢复程序

系统恢复是指在系统由于故障而不能工作之后将系统带回到正常操作的处理。目标是减少宕机时间、数据丢失和对其它系统的负面影响。

注册管理机构应满足以下要求:

- a) 对发生在注册管理机构系统不同部分的故障使用恢复程序,例如:
 - 1) 数据中心故障;
 - 2) 数据库故障;
 - 3) 服务器故障;
 - 4) 网络故障。
- b) 利用冗余和高可用注册管理机构体系帮助从这些故障中迅速恢复过来;
- c) 使用数据库备份和异地容灾机制实现故障的恢复;
- d) 提供每种类型故障恢复的时间统计;
- e) 将每一个系统运行中断记入日志,并将可能导致运行中断的系统问题记录在案。

8.2.1.7.3 技术和其它支持

注册管理机构可给注册服务机构提供多层次的电话支持。

注册管理机构可给注册服务机构、注册人和互联网用户提供基于web的支持。Web的内容可包括知识背景、FAQ、注册服务机构工具箱、白皮书和电子邮件消息。

8.2.1.8 服务水平要求

对Tier 1注册管理机构操作方面的服务水平要求包括以下方面:

- a) 注册管理机构数据库吞吐量-每秒钟的事务处理数;
- b) 注册管理机构数据库可用性;
- c) 注册服务机构帐户数;
- d) 并发的注册服务机构-注册管理机构连接数;
- e) 区文件生成的频率:每天、小时、分钟的速率;

- f) 区文件传播时延：分钟、秒；
- g) 需要的域名服务器数量；
- h) ContactInfo 数据库生成的频率：每天、小时、分钟的速率；
- i) ContactInfo 查询响应时间；
- j) ContactInfo 查询吞吐量-每秒的查询数量；
- k) ContactInfo 数据库可用性。

具体指标待定。

8.2.1.9 Tier1 系统的性能要求

8.2.1.9.1 DNS 服务

8.2.1.9.1.1 性能

DNS查询往返的时间不超过300ms。

8.2.1.9.1.2 可用性

- a) 在抽样期间如果对DNS查询的响应满足以上性能规定的占有所有在抽样期间测量的事务处理的95%,则认为该DNS PoP (Point of Presence) 可用。
- b) 如果在抽样期间发出的查询中有99%以上在以上性能规定中规定的往返响应时间之内得到响应,则该DNS服务被认为在该抽样期间可用。
- c) 在每个日历年, SRS系统的不可用总和应不超过5分钟,它代表了99.999%的系统可用性。在超过一半以上系统的SRS PoPs时间应没有并发的计划内的SRS业务系统中断。
- d) DNS域名服务系统的不可用总和为0,即DNS域名服务应具有100%的可用性。在超过一半以上系统的DNS域名服务PoPs时间应没有并发的计划内的DNS业务系统中断。
- e) 域名服务器应具有超过99.99%的可用性。

从星期一0000GMT开始的每个日历周内,计划内的系统中断应不超过4小时,每个月的总量不超过8小时。由于主系统或软件升级(扩展的计划内的系统中断),每个月Tier 1注册管理机构可有一次额外的计划内的系统中断,不超过每个月8小时。在有扩展的计划内的系统中断发生的月份,不可以发生其它计划内的系统中断。

8.2.1.9.1.3 更新

在所有的更新中应有95%的DNS服务的更新时间不超过5分钟。

8.2.1.9.1.4 跨网域名服务器性能(CNNP)要求

对跨网服务器性能的要求是所测量的往返时间,即从发送DNS查询请求给Tier 1域名服务器到收到Tier 1域名服务器的响应时间,应小于300ms以及所测量的分组丢失率,即没有收到响应分组的百分比应小于10%。

8.2.1.9.2 EPP 性能

增加、修改和删除命令的性能规定为3000ms。测量从命令完全收到开始,到命令完全发出为止。

检查命令的性能规定为1500ms。测量从命令完全收到开始,到命令完全发出为止。

对于从一个注册服务机构传送到另一个注册服务机构的请求,允许额外的验证时间。

8.2.1.10 Tier1 系统的安全性要求

8.2.1.10.1 运营系统的安全性

Tier 1 注册管理机构、SRS 和域名服务器数据中心面临着各种各样的安全性威胁,包括欺诈、非法闯入、数据修改、拒绝服务、以及对设备的物理攻击。此外,由于 Tier 1 注册管理机构包含来自互相竞争的注册服务机构拥有的数据,安全性程序必须包含用户鉴权程序,以确保每一个注册服务机构的文件只有该注册服务机构授权的人才能够使用。如果不注意这些安全性的威胁,可能会导致计划外的宕机时间和破坏,或者是拒绝服务。

Tier 1注册管理机构应满足以下要求:

- a) 综合分析注册管理机构系统可能面临的威胁,并指出易受攻击处以及安全性攻击的类型;

- b) 基于所进行的分析,该注册管理机构应该加强为注册管理机构系统的各个部分提供安全性保护的多层次程序,包括:
- 1) 对ContactInfo和DNS应用的保护;
 - 2) 在服务器操作系统处的控制接入;
 - 3) EPP、ContactInfo和客户服务应用的应用层安全性特征;
 - 4) 网络连接安全性;
 - 5) 数据库安全性;
 - 6) 闯入的检出;
 - 7) 用户标识和鉴权;
 - 8) 操作的连续性;
 - 9) 物理的安全性。

注册管理机构应该对上述各方面规定使用的安全性机制以及可相应防护的攻击类型。

所采取的安全性措施应基于相关标准,包括现存的IETF标准(IPSec, PKI和SSL),以及正在演进的IETF关于EPP和DNSSec方面的标准。

8.2.1.10.2 DNS 安全性

- 建议使用事务处理签名(TSIG)协议进行Tier1或Tier2的主从域名服务器之间的所有的数据传送。
- 建议使用DNSSec提供对数据来源的鉴权。
- 除了DNS服务器软件之外,DNS服务器应该运行最小集合的应用和系统业务。
- 定期对所有DNS服务器进行检查以确保数据的一致性。

8.2.1.10.3 协议安全性

- 必须使用TLS[RFC 2246]协议以保证传送层的安全性,从而部分提供SRS应用的安全性。
- 应使用TLS对每一个EPP会话进行鉴权和加密。ENUM注册管理机构应使用商业认证权威机构颁发的X.509服务器证书以及ENUM注册服务机构密码对每一个EPP客户连接进行鉴权。

8.2.1.10.4 物理安全性

- a) Tier 1注册管理机构应该使用各种物理安全系统以确保未经授权的人员不得接入那些敏感的设备 and/或数据。
- b) 所有的包含敏感数据的服务器应该保证物理上的安全性,应保证只有一个受控制的人员列表能够获得接入权。
- c) 未经授权的人员不得接入内部网络。所有的内部网络与公共接入分离,对外部的互联网链路设置防火墙保护,防止入侵者获得接入。
- d) 上述的安全性措施将不干扰授权人员对数据中心的24小时接入。
- e) 一个ENUM Tier 1注册管理机构应至少有2个主从域名服务器。

8.2.1.10.5 网络安全性

- a) 对于所有受限制的业务(包括除DNS解析、ContactInfo查询以外的其它业务)都要求用户标识、密码和IP地址范围的检查。
- b) 在ENUM注册服务机构和Tier 1注册管理机构之间的所有文件传送都应该使用安全的文件传送协议[RFC 2228 FTP Security Extensions、RFC 2577FTP Security Considerations或其他等同的协议]。
- c) 系统维护应通过SSH或类似的安全连接进行。不应该在DNS网络的任何系统上操作Telnet服务器,否则可能会给这些系统带来安全性风险。
- d) 在与DNS、ContactInfo、FTP、和WWW 服务相关的各部分中,每一个系统应该仅能操作一个非常有限的基本业务集合。应设置防火墙为系统硬件提供保护,且设置IP过滤规则集合,拒绝不合适的分组。

- e) 对于限制IP的业务, 应该对每一个IP地址做出规定, 而不能使用网络地址段(network address)。因为使用网络地址段可能会出现某个主机冒充使用内部网络的一个空余IP地址的情况。
- f) “分组取样器”可对通过一个网络接口的所有流量进行检查, 应在适当位置放置分组取样器捕捉可疑的流量。这样可以积极地扫描不正确的或非法的分组, 以发出警报。分组取样器还可以提供一些攻击来源的指示, 可用于将来防止该攻击的发生。
- g) 通过安全性监听程序验证网络的安全性。安全性监听程序将从一个与互联网相连的主机对由Tier 1注册管理机构操作的服务器的所有TCP和UDP端口进行扫描。
- h) DNS服务器应完成安全性测试, 且要对相应的报告进行定期审核。每一次测试都应该尝试使用特殊攻击方式测试系统的安全缺陷, 并报告测试的结果。测试中可尝试进行以下攻击:
 - 1) 缓冲器溢出;
 - 2) 丢失格式串;
 - 3) 分割包攻击;
 - 4) 数据洪水;
 - 5) DNS欺骗;
 - 6) FTP欺骗;
 - 7) 字典密码;
 - 8) 重放攻击;
 - 9) 拒绝服务。

当发现新的弱点、安全性缺陷或技术时, Tier 1注册管理机构应该更新所使用的测试, 应根据来自于与安全性相关的邮件列表、网站、新闻组的信息以及业界最好的实践经验进行更新。

8.2.1.10.6 备份安全性

应通过安全的网络对主要的Tier 1注册管理机构站点进行备份。在实施过程中, 建议Tier 1注册管理机构应该对敏感数据的备份使用加密方案。安全清理人员应将删除的媒体传送至安全的位置, 并在该处存储和维护, 以便以后可以恢复使用。

8.2.1.10.7 客户服务人员接入

应该将所有的客户服务代表(CSR)接入限制在一个特定的网络子网(子网过滤)范围内。目的是阻止互联网上任何地点的黑客猜测CSR的用户名/密码并进入系统。

在登录屏幕上输入有效的CSR用户名和密码之后, 任何时候都要根据可识别的IP地址的集合进行最终的验证。如果有人提供了有效的用户名和密码但是没有从有效的IP地址登录, 则不允许他们登录, 同时也不向他们说明原因。

8.2.1.10.8 安全监听和报告

Tier 1注册管理机构将进行合理的安全性监听, 以测试所有系统的配置问题和安全漏洞, 并将根据监听的结果定期形成安全性报告, 在报告中将给出具体的系统改造建议以及实施补救措施的时间表。

所有的安全性入侵都将报告给负责安全性的管理部门。如果检出了一个严重的入侵, 在必要时有些业务可能被暂停, 以确保Tier 1注册管理机构数据的可靠性。

8.2.2 Tier2 系统的要求

Tier 2系统的主要功能是存储ENUM注册人的NAPTR记录信息。

8.2.2.1 与其它功能实体的交互作用

8.2.2.1.1 Tier2 提供者--ENUM 注册服务机构

Tier 2提供者给ENUM注册服务机构提供Tier 1域名服务器的信息, 以便注册服务机构与Tier 1进行通信。

注册服务机构给Tier2提供者提供NAPTR记录信息。

将注册服务机构从Tier1得到的信息通知Tier2提供者，例如：编号计划变更、联络信息或者是其它的信息。

8.2.2.1.2 Tier2 提供者—ENUM 注册人

通过Tier 2提供者与ENUM注册人之间的交互作用完成以下功能：

帐户的管理（生成、关闭、修改和计费）；

注册人给Tier 2提供者提供NAPTR记录信息；

注册人授权ASP直接与Tier 2提供者进行交互作用。

8.2.2.1.3 Tier2 提供者—ASP

ASP管理存储在Tier 2提供者中的NAPTR记录信息。

8.2.2.2 性能要求

8.2.2.2.1 DNS 服务响应时间

对于一个ENUM查询返回NAPTR记录的时间要求是：

——95%的查询在1秒钟内返回NAPTR记录；

——99%的查询在2秒钟内返回NAPTR记录。

在Tier1的响应时间为300ms的情况下，假设Tier1的信息已经被缓存，对于Tier2有如下要求：

——95%的查询在700ms内响应；

——99%的查询在1700ms内响应。

考虑到PSTN的要求，建议Tier2应满足有95%的查询在500ms内响应的要求。

8.2.2.2.2 DNS 服务可用性

每年系统中断时间少于5分钟；或者是具有99.999%的可用性。

8.2.2.3 安全性要求

同8.2.1.10。

8.2.3 用户隐私信息的保护

在ENUM的实施Tier 1注册管理机构、Tier 2提供者、注册服务机构应该注意用户隐私信息的保护。

在ENUM的实施Tier 1注册管理机构、Tier 2提供者、注册服务机构应该遵守以下原则：

- a) ENUM注册服务机构可能会收集与注册人相关的各种业务的URI，注册人希望能够通过ENUM将这些URI与其电话号码关联起来，而在对ENUM查询做出响应时，需要透露这些URI。由于这种透露是ENUM操作的一个组成部分，因此这样的使用和透露是不能限制的。由于这种透露是ENUM操作的一个基本组成部分，因此需要向注册人说明这种情况。
- b) 在收集与注册人相关的信息时，应该给注册人清晰、明确的通知，包括收集了什么信息，如何收集这些信息（例如通过直接方式或者是通过不明显的方式，例如cookies），是否将收集到的信息透露给其他实体，以及是否有其他实体通过他们收集信息等。
- c) 注册人有权拒绝对与他相关的数据进行某种类型的收集/使用。
- d) 注册人有权接入被收集的与他相关的数据。应该向每一个注册人提供到与该注册人相关的信息的合理接入，但这种接入不应该给任何一方带来高昂的代价和繁琐的操作，避免过重的负担和花费。例如，可以采用密码保护方式的web接入。
- e) 保证注册人的数据不会被未经授权接入。
- f) 注册人有权要求更正与其相关的不准确的信息和/或删除与其相关的信息。为了保证ENUM的正常运行，NAPTR记录必须保持是最新的。注册人有权更改其他的信息，特别是在ENUM注册过程中使用的信息，例如地址、账单信息、用户名或密码。
- g) 对于个人数据的使用将限于一些与收集这些数据的目的相关的规定的用途。没有注册人的明确同意，既不能将数据透露给其他方，也不能将其用于实现和维护ENUM注册之外的其他用途。
- h) 对数据只保留一段合理的时间，当不再需要实现和保持ENUM注册时，相应的数据应不再保存。

- i) Tier1的注册管理机构收到基于类似WHOIS协议的ENUM域名查询时,应返回为该域名服务的注册服务机构的联络信息,而不是注册人的联络信息。如果需要联络,注册服务机构将与注册人进行联络,并将问题报告转给注册人或者是注册人指定的联系人。在注册人有欺诈和违法活动时,注册服务机构将向相应的权威机构透露注册人的信息。

9 注册管理要求

9.1 ENUM 的提供模式

ENUM的提供模式如图5所示:

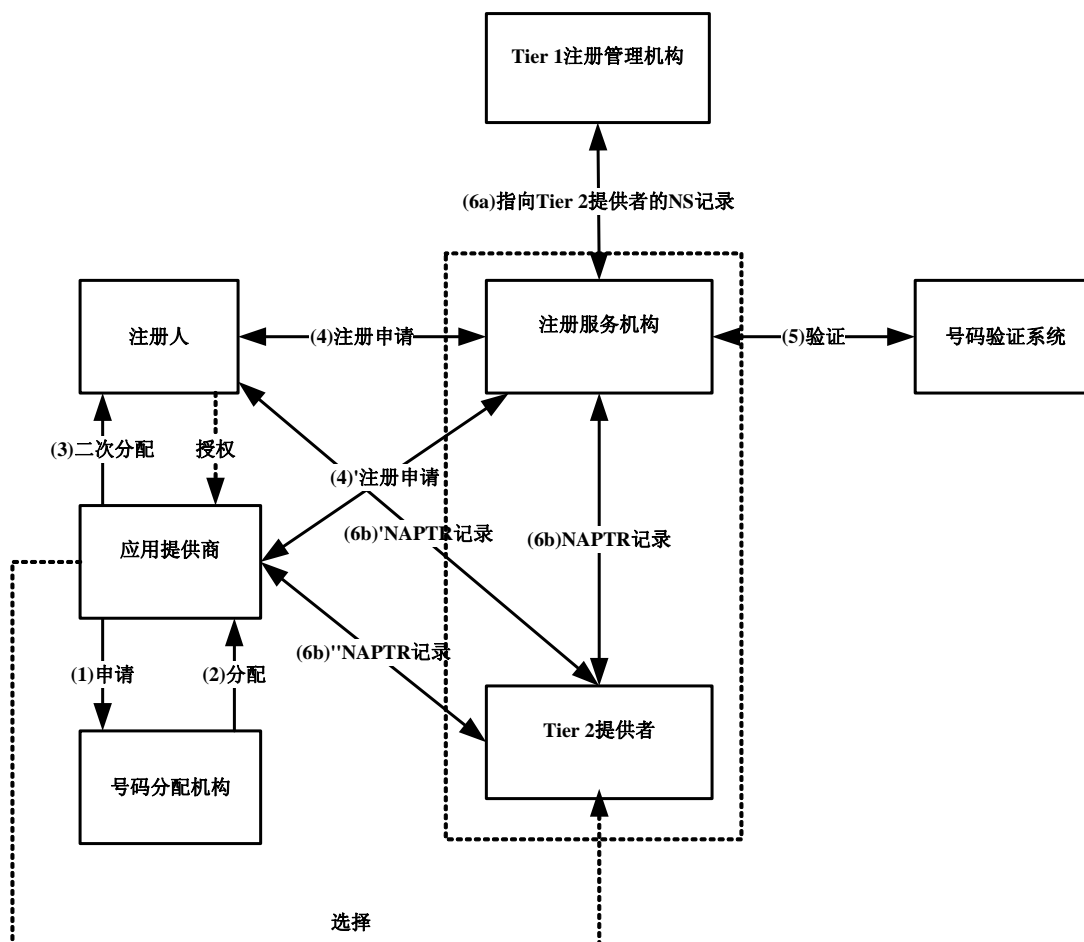


图5 ENUM 的提供模式

ENUM应用提供商从ENUM号码分配机构获得了号码资源后,再将该号码资源二次分配给ENUM用户。获得号码资源的ENUM用户可以选择一家ENUM注册服务机构完成注册,也可以授权应用提供商,由应用提供商选择一家ENUM注册服务机构完成注册。注册服务机构接到注册人的注册申请后,需通过号码验证系统对注册人的注册申请进行验证,验证通过后注册服务机构将向Tier1注册管理机构提供NS记录,这些记录指向注册人指定的Tier2提供者。根据注册人的选择,可由注册人、注册服务机构或应用提供商向Tier 2提供者提供NAPTR记录。注册服务机构还可以直接提供或者通过外包的方式提供Tier2功能。

在ENUM的提供过程中主要涉及以下实体:

a) 注册人

注册人是指将他的电话号码注册到ENUM中的用户,他可以选择一个注册服务机构来为他完成注册,并且选择一个Tier 2提供者负责保存该用户电话号码的NAPTR记录。当注册人终止与其电话号码

相关的电话业务时,注册人负责取消注册。注册人与注册服务机构之间的接口有多种形式(Web、电话或书面邮件等),该接口是非标准化的,由注册服务机构选择。

注册人也可以直接与Tier 2提供者之间进行交互作用,它们之间的接口也不是标准化的,可根据双方之间的协议确定。

b) 注册服务机构

注册服务机构负责接收来自注册人的注册请求,然后对注册人是否有权注册相应的号码进行验证,如果请求有效,注册服务机构将与Tier1注册管理机构接口,请Tier1注册管理机构在他的域名服务器中建立一个指向该注册人的Tier2域名服务器的指针。

注册服务机构还可以直接提供或者通过外包的方式提供Tier2功能。注册服务机构可与注册人选定的Tier2提供者或应用提供商之间交互,代表注册人提供NAPTR记录。

注册服务机构与Tier1, Tier2注册管理机构之间的接口是标准化的接口,采用EPP协议。

注册服务机构负责周期性地对已经完成的注册进行重新验证,并终止没有通过有效性验证的注册。

ENUM注册服务机构需要与Tier 1注册管理机构建立信任的关系,即需要有安全的通信方式, Tier 1注册管理机构需要为注册服务机构分配用户ID和密码用于会话管理,为注册服务机构分配注册服务机构标识用于ENUM注册标识,并且在ENUM开始注册之前交换联络和其他信息。

c) Tier 1注册管理机构

Tier1注册管理机构负责一些授权的域名服务器,这些服务器中存储相应的信息,指示哪些Tier 2提供者持有与注册到ENUM中的电话号码对应的NAPTR记录。注册管理机构的域名服务器将对ENUM DNS查询做出响应,提供相应的Tier 2主机名。

Tier 1注册管理机构接受来自注册服务机构的注册申请,并且在发生争议时进行管理和处理。

Tier 1注册管理机构与注册服务机构进行交互作用,他们之间通过EPP协议接口。

Tier 1注册管理机构还与Tier 0注册管理机构交互作用(经过电信主管部门的批准),以从Tier 0处获得对本国号码的授权。

建议Tier 1注册管理机构不能同时兼做注册服务机构。

Tier 1注册管理机构将是由电信主管部门指定的机构。

d) Tier 2提供者

Tier 2提供者对所服务的号码的ENUM查询提供响应,它将提供与所查询的号码相对应的NAPTR记录的集合。

Tier 2提供者负责提供ENUM注册人或者是ENUM注册人授权的机构(例如ASP,注册服务机构)根据所签署的商业协议请求的NAPTR记录。在涉及多个ASP的情况下, Tier 2提供者必须确保NAPTR记录中的“顺序(order)”域和“优先(preference)”域正确地反映出注册人的选择。

Tier 2提供者负责提供Tier 2域名服务器,并向注册服务机构提供技术联络信息,以便注册服务机构将该信息传递给Tier 1注册管理机构。如果域名服务器或联络信息发生变更,由Tier 2提供者负责通知注册服务机构。

由于ENUM Tier2提供者将存储用户的通信联络信息,因此只有经过电信主管部门资质认可的机构才能够作Tier 2提供者,可以是应用提供商,也可以是ENUM用户自己。

e) 验证系统

图6中的验证系统将对注册申请者是否拥有相应的电话号码,以及该电话号码是否被停用等进行验证,该验证系统可由ENUM应用号码的分配者提供,也可由第三方中立机构提供。

f) 应用提供商

应用提供商为用户提供各种业务应用,在提供这些业务和应用的过程中可能需要利用存储在Tier 2服务器中的用户信息。应用提供商包括提供ENUM应用的电话运营商。

9.2 国家码的注册

我国国家码“86”的注册需经电信主管部门批准,并按照相关规定提出申请。

9.3 用户号码的注册

用户号码的注册由注册人或者是注册人授权的应用提供商选择注册服务机构完成。以下流程适用于注册人通过注册服务机构注册ENUM的情况，由注册服务机构负责选择合适的Tier 2服务提供者，并代理用户注册，注册服务机构不作Tier 2提供者。

9.3.1 注册

注册流程如图6所示：

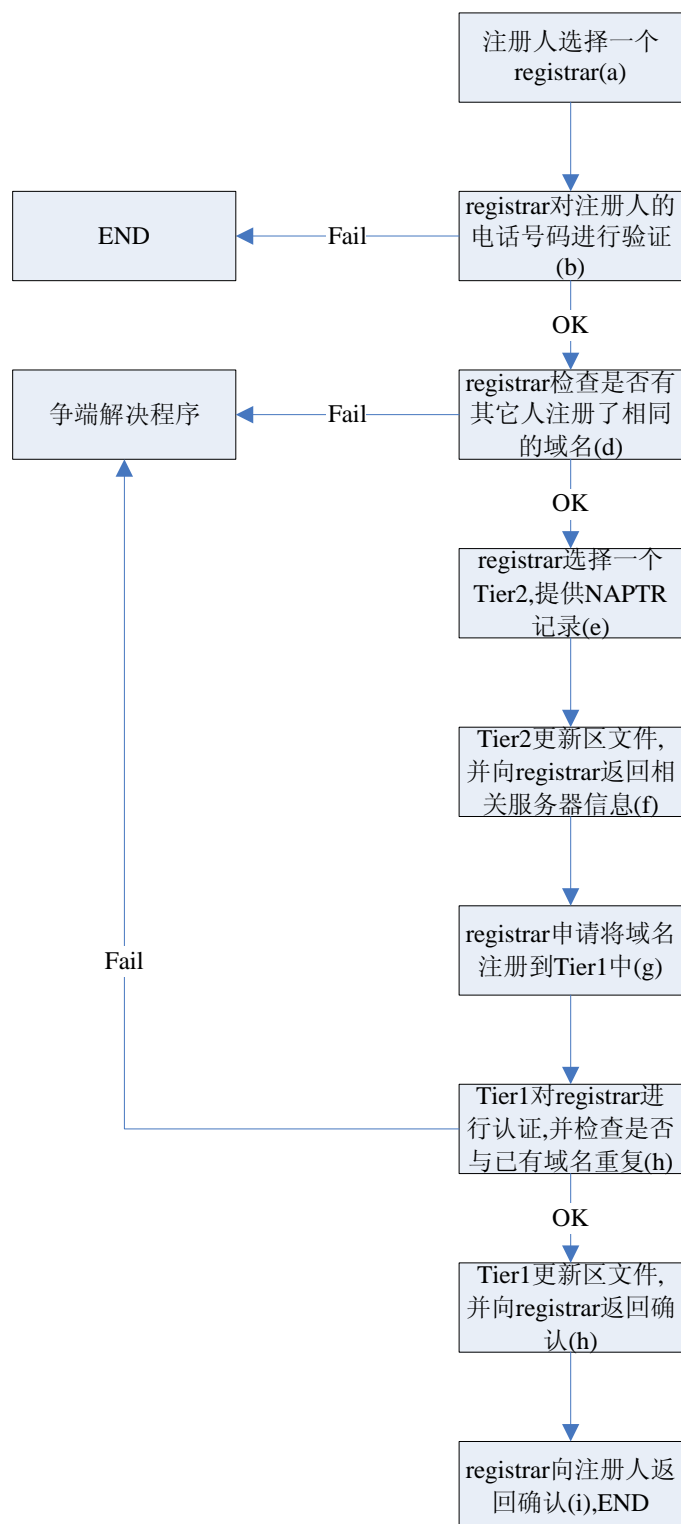


图6 注册人注册流程

- a) 注册人选择一个ENUM注册服务机构，并向其提供以下信息：
 - 1) 电话号码；
 - 2) ENUM注册期限（例如2年）；
 - 3) 注册人的信息，以及管理和计费方面的联络信息；
 - 4) 应用相关信息（应用/业务类型，比如：E-mail地址，SIP，fax，TN，和URLs）及用户希望的业务优先级；
 - 5) ENUM注册服务机构需要的认证、鉴权和管理（AAA）信息。
- b) 如果有必要，ENUM注册服务机构应与注册人进一步沟通以获取更多信息。然后，ENUM注册服务机构将对用户的电话号码进行有效性的验证；
- c) 如果号码有效性验证失败，则注册人的申请被拒绝，流程终止；
- d) 如果号码有效性验证成功，ENUM注册服务机构将检查是否有其他的注册人已经注册了相同的ENUM域名。如果有，本流程终止，启动争议解决程序。如果没有，注册服务机构继续执行第e)步操作；
- e) ENUM注册服务机构选择合适的Tier 2提供者，并向该Tier 2提供者提供以下两种信息之一：
 - 1) 命名权威指针（NAPTR）资源记录；或
 - 2) 如果Tier 2提供者可以完成NAPTR记录的格式化，那么注册服务机构提供
 - 电话号码或ENUM域名；
 - 与应用相关的信息（例如：应用/业务类型，E-mail地址，SIP，fax，电话号码，和URLs。
- f) Tier 2提供者将用户的记录注册到至少两个域名服务器中，并且在服务器中将该ENUM域名更新到区文件中，并向ENUM注册服务机构返回以下信息：
 - 1) 与ENUM域名相关的服务器主机名称列表；
 - 2) ENUM域名技术联络方的联络信息。
- g) ENUM注册服务机构向Tier 1注册管理机构提供以下信息，将ENUM域名注册到Tier 1注册管理机构中：
 - 1) 提交新ENUM域名的注册申请；
 - 2) 期望注册的ENUM域名（例如：0.9.8.7.6.5.4.3.2.1.y.x.1.e164.arpa）；
 - 3) 一个域名服务器主机名的列表；
 - 4) ENUM业务注册期限（比如：2年）；
 - 5) ENUM注册人的联络信息以及技术方面、管理方面、计费方面的联络信息。
- h) Tier1注册管理机构通过对ENUM注册服务机构的认证和鉴权后，检查申请中的域名是否与已存在的域名重复。
 - 如果与已存在的域名重复，则启动号码分配争议处理程序，本进程结束；
 - 如果不与已存在的域名重复，Tier1注册管理机构将回复ENUM注册服务机构，告知ENUM域名注册已经被接受以及该注册的有效期。并且Tier1注册管理机构将更新域文件，将新的ENUM域名添加到域名服务器的记录中。完成域文件更新后，DNS就可以实时的查询该域名指向的Tier2域名服务器的指针。
- i) ENUM注册服务机构收到Tier1注册管理机构注册成功的确认后，通知申请ENUM业务的用户ENUM业务注册成功。

9.3.2 注册人终止 ENUM 注册

注册人终止ENUM注册流程如图7所示：

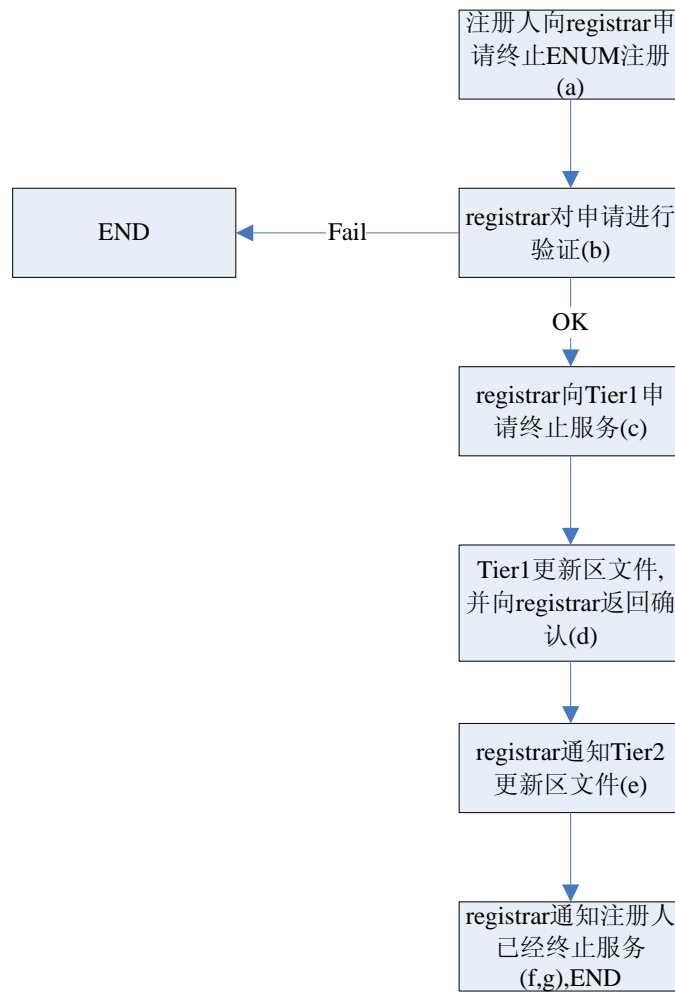


图7 注册人终止注册流程

- a) ENUM注册人与ENUM注册服务机构联系表明希望终止他/她的ENUM域名注册。ENUM注册人提供以下信息：
 - 1) ENUM电话号码；
 - 2) 终止ENUM注册的申请；
 - 3) ENUM注册服务机构所需的认证，鉴权和管理（AAA）相关信息。
- b) ENUM注册服务机构检查该申请是否来自授权的ENUM注册人

如果是，ENUM注册服务机构提醒ENUM注册人终止他/她的ENUM注册可能会导致相关的地址和业务可能不能象以前那样使用了，然后执行c)；

如果不是，注册服务机构告知申请者他/她无权终止相关ENUM域名的业务注册，终止处理流程。
- c) ENUM注册服务机构提供以下的信息，通知Tier 1注册管理机构终止相关的服务：
 - 1) ENUM域名；
 - 2) 终止ENUM的申请；
 - 3) Tier 1注册管理机构所需的认证、鉴权和管理（AAA）相关信息。
- d) Tier 1注册管理机构通知ENUM注册服务机构相应的ENUM域名注册已被终止，并将该ENUM注册从本地数据存储器 and 域名服务器中删除。
- e) ENUM注册服务机构告知ENUM注册人终止注册已成功完成。
- f) ENUM注册服务机构通知Tier 2提供者从它的域名服务器中删除相应的NAPTR记录，以终止服务。
- g) 如果注册人授权应用提供商可以接入/更改Tier 2提供者中的数据，注册人应通知应用提供商ENUM注册已经终止。

9.3.3 争议解决程序

a) 可能触发争议解决程序的情况

以下三种情况可能会触发争议解决程序：

- 1) 注册服务机构通知注册人申请注册的E. 164号码已经注册；
- 2) 注册服务机构在试图将相应的E. 164号码注册到Tier 1注册管理机构中时，由于该号码已经注册遭到Tier 1注册管理机构的拒绝；
- 3) 被分配了E. 164号码的用户通过其它的方式（例如：进行ENUM DNS查询）发现该号码已经注册到Tier 1注册管理机构中了。

b) 争议的提出

注册服务机构通知ENUM注册人相应的E. 164号码已经被注册时，该ENUM注册人可通过电子邮件或邮寄的方式向负责该号码的Tier 1注册管理机构提交争议解决申请表。如果是被分配了E. 164号码用户通过其它的方式发现该号码已经在Tier 1注册管理机构中注册，即便该用户不想注册该号码，只是想将已经存在的注册从注册管理机构中删除，他/她也可以通过电子邮件或邮寄的方式向负责该号码的Tier 1注册管理机构提交争议解决申请表。

c) 授权方的确定

由Tier 1注册管理机构对发生争议的各方进行验证，并找出真正对相应E. 164号码有权的用户。可使用在注册初始阶段注册服务机构使用的方式。在验证过程中，Tier 1注册管理机构将需要从发生争议的各方获得具体的标识信息和分配信息。当明确了争议各方中最合法的注册用户后，在维护合法用户的准则下，取消非法方的注册请求或变更非法方的注册。

所有注册实体，注册服务机构和用户都应接受并使用的争议处理程序。争议处理程序可在每个用户注册ENUM业务时附在用户签署的用户协议中。

10 协议要求

ENUM提供和解析过程中所涉及的协议如图8所示。

在对由E. 164号码转换的域名进行解析的过程中，建议使用DNSSec协议。

在为用户提供ENUM应用的过程中，注册人使用安全的协议与注册服务机构接洽，建议使用HTTPS，HTTPS使用SSL提供安全性机制。在注册服务机构和验证系统之间，建议使用HTTPS对注册人进行验证，在初期也可选择通过电话、传真或书面邮件等形式认证。

在注册服务机构与Tier-1和2的数据库之间建议使用EPP。

在互为备份的两个Tier-2数据库之间建议使用IXFR/AXFR方式进行同步，同步消息使用TSIG或者SIG (0) 协议进行安全加密，同步使用的FTP文件建议使用采用IDEA或3DES加密算法加密。

ENUM应用的典型消息流程见附录D。

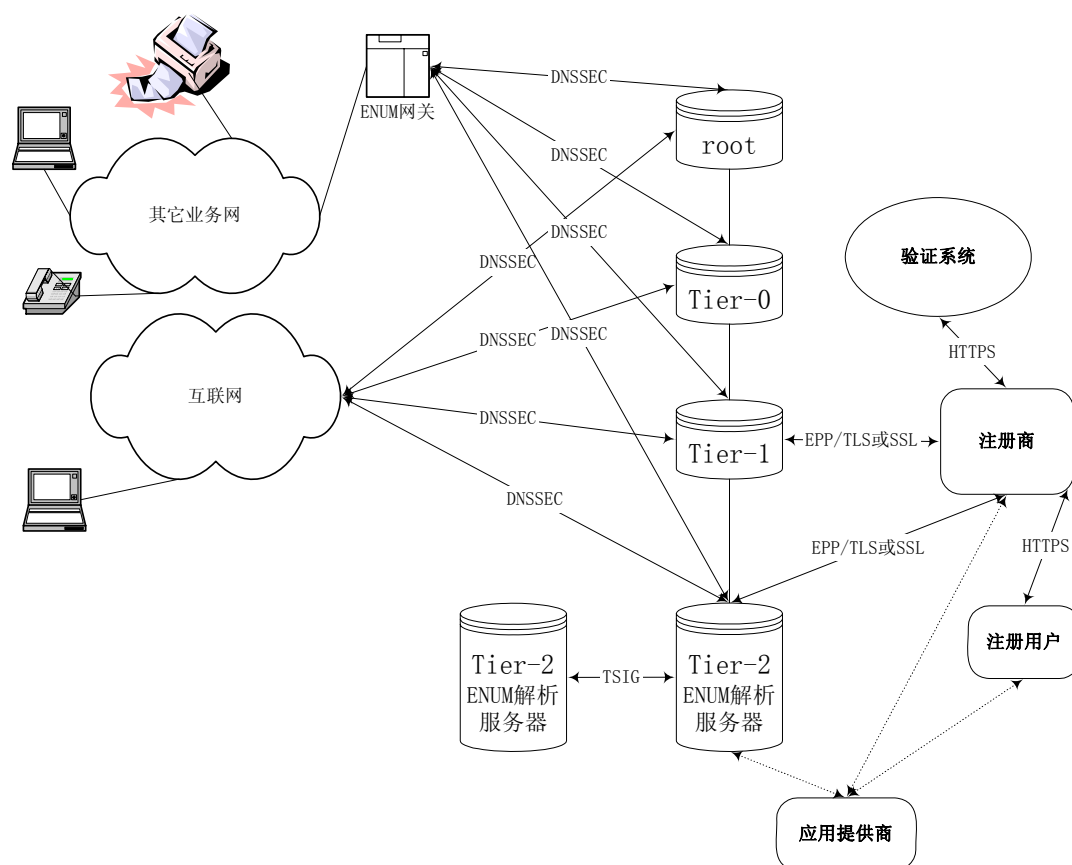


图8 ENUM 提供和解析过程中所涉及的协议

10.1 DNSSEC

DNSSEC (DNS安全性扩展)在普通DNS服务的基础上,增加了数据初始认证和数据完整性认证。该认证过程就是支持DNSSEC的解析器根据密钥(通过交互获得的公钥或者配置的共享密钥)和某种解密算法,对支持DNSSEC的服务器返回的带有数字签名(或者含有密钥的摘要)的应答进行认证的过程。为了支持DNSSEC,普通的DNS服务器和解析器都需要增加相应的资源记录 and 加密解密算法(或者摘要算法)。该协议的主要内容见附录A,具体要求见RFC 4033、RFC4034、RFC4035。

10.2 HTTPS

Hypertext Transfer Protocol(超文本传输协议)是因特网上 www 的客户端和服务端之间主要的协议,由于 web 的简单易用使其成为因特网上很多 client/server 应用的主要框架。但是,在目前的很多应用中,客户端和服务端要能够秘密交换一些敏感的数据,而原来的 HTTP 协议对此的支持是明显不够的。

HTTPS(HTTP over TLS)是在传输层(如 TCP)之上增加一层 TLS 协议,利用 TLS 来传输 HTTP 协议,以此来保证 HTTP 传输的安全性。

该协议的具体内容见RFC 2818。

10.3 EPP

EPP 是由有状态的 XML 描述的可运行于多种传输层协议之上的协议,它提供四种基本服务元素:业务发现、命令、响应和扩展框架,该框架支持对被管理的对象进行定义,并对这些对象的协议请求与响应之间的关系进行定义。

利用EPP提供的扩展规则,可将协议操作的定义放置在特定对象的内容中,在不修改基本协议的情况下,提供添加新对象映射的能力,达到对协议扩展的目的。使用EPP实现提供和管理存储在共享中心

数据库中因特网域的机制称为EPP域名映射 (EPP Domain Mapping)。该映射使用XML定义应用于域名的EPP命令语法和语义。EPP E. 164号码映射是对EPP域名映射的扩展，添加了有关E. 164号码相关的内容，该映射使用XML定义应用于E. 164号码的EPP命令语法和语义，该协议的主要内容见附录C，具体要求详见RFC 3730、3731、4114。

10.4 TSIG

TSIG的全称为DNS的密钥事务认证 (Secret Key Transaction Authentication for DNS)，该协议允许使用共享密钥和单向哈希进行事务层的鉴权。它可被用于对来自认可的客户的动态更改进行鉴权，或对来自认可的递归名字服务器的响应进行鉴权。

该协议的主要内容见附录B，具体要求见RFC2845。

10.5 IXFR/AXFR

IXFR的全称为增量区传送 (Incremental Zone Transfer)，AXFR的全称为完整区传送 (All Zone Transfer)，该协议是在DNS协议之上的协议，提供Tier-2数据库之间同步的机制。

该协议的具体内容参见RFC1995。

附录 A

(资料性附录)

DNSSEC 协议

DNSSEC(DNS 安全性扩展)在普通 DNS 服务的基础上,增加了数据初始认证,完整性保护和经认证的数据拒绝。该认证过程就是支持 DNSSEC 的解析器根据密钥(通过交互获得的公钥或者配置的共享密钥)和某种解密算法,对支持 DNSSEC 的服务器返回的带有数字签名(或者含有密钥的摘要)的应答进行认证的过程。为了支持 DNSSEC,普通的 DNS 服务器和解析器都需要增加相应的资源记录和加密解密算法(或者摘要算法)。

DNSSEC中增加了四种资源记录类型:资源记录签名,DNS公钥,授权签名者和下一个安全记录(RRSIG, DNSKEY, DS和NSEC),并增加了两个消息头比特:禁止检查和已认证数据(CD和AD)。位置支持因为增加了DNSSEC记录而增加的DNS消息长度,DNSSEC还要求支持EDNS0。

A.1 概念

A.1.1 资源记录(RR, Resource Record)

在 DNS 系统中,和一个域名相关的信息的集合,具体格式请参考[RFC1034]。

DNSKEY RR: DNSSEC的一种资源记录,用于保存公钥。

RRSIG RR: DNSSEC的一种资源记录,用于保存数字签名。

NSEC RR: DNSSEC的一种资源记录,用于说明区中存在哪些域名及资源记录类型。

DS RR: DNSSEC的一种资源记录,用于保存一个DNSKEY RR的哈希摘要,且该资源记录只存在相关DNSKEY RR所属区的父区。

A.1.2 资源记录集(RRset)

具有某部分共同属性(一般指相同的域名,类别和类型)的资源记录的集合。

A.1.3 认证链(authentication chain)

交错的DNS公钥(DNSKEY)资源记录集和授权签名(DS)资源记录集组成了签名数据的认证链。在DNSSEC里,通过DNSKEY RR对DS RR的签名的验证,可以证明该DS RR是可信的。而DS RR中包含了另一个DNSKEY RR的哈希摘要,通过检查这个新的DNSKEY RR的哈希摘要是否和DS RR的内容匹配,可以检查新的DNSKEY RR是否可信。反过来,这个新的DNSKEY RR可以认证另一个DNSKEY RRset,而这个集合中的某个DNSKEY RR可以用来认证另一个DS RR,这样循环下去,直到完成对目标DNSKEY RR的认证,该目标DNSKEY RR可以用来验证一个普通的DNS的资源记录。

比如,根域的DNSKEY RRset可以用来认证"example."域的DS RRset,而"example."域的DS RRset包含了"example."域某个DNSKEY的哈希摘要,而和这个DNSKEY相对应的私钥对"example."域的DNSKEY RRset进行签名,这个私钥还对"www.example."域的RR和"example."的某个有权子域如"subzone.example."的DS RRs进行签名。

A.1.4 信任起点(Trust Anchor)

在认证链中,每个节点的认证都是依赖于上一个节点,因此递推下去,认证链的第一个起点必须是安全的并且是不需要认证的,这个起点就称作信任起点。在DNSSEC中,信任起点是一个已经配置的DNSKEY RR或者DS RR,后者是一个DNSKEY RR的哈希摘要。一般的说,解析器不会通过DNS协议而是通过其他安全的方法来获得Trust Anchor的值。

如果Trust Anchor 是一个ZSK(区签名密钥),则解析器会用这个密钥来认证某个区的数据;如果Trust Anchor 是一个KSK(对密钥签名的密钥),则解析器会用这个密钥来认证ZSK;如果Trust Anchor

是一个密钥的哈希摘要，则解析器必须先通过DNS协议来获得这个密钥。为了能够使解析器建立信任链，服务器会将一个公钥的签名和这个公钥本身一同发送。

因此，简单的说，认证链可以如下表示：DNSKEY→[DS→DNSKEY]*→RRset，其中“*”表示0个或多个。

A. 1.5 对密钥签名的密钥(KSK, key signing key)

通常“对密钥签名的密钥”会对“区签名密钥(ZSK)”签名，该“区签名密钥”会对区中的其他数据签名。一般要求“区签名密钥”经常更换，但是“对密钥签名的密钥”则会很长时间有效。

一般的，对一个区的认证公钥（一个或者多个）需要一个私钥对其签名，和这个私钥对应的认证公钥就是“对密钥签名的密钥(KSK)”。而和这个区的认证公钥（称之为ZSK）相对应的私钥是对这个区的其他数据进行签名的。一般要求“区签名密钥”经常更换，但为了能有一个区的安全入口，“对密钥签名的密钥”会长时间有效。

A. 1.6 区签名密钥(ZSK, Zone Signing Key)

对一个区数据进行签名的私钥所对应的认证公钥。

A. 1.7 消息验证码(MAC)

发送方通过密钥和某一算法将某一明文转换成某一固定长度的密文，并将该密文同明文一起发送，拥有相同密钥的接收者按照同样的算法能够将该明文转换成同样的密文。对于接受者来说，该密钥只有发送者拥有，因此当接收到的明文和密文匹配时，可以认为该消息从特定的发送者发出，实现了对发送方的认证，这样的密文称为MAC。

A. 2 DNSSEC数据认证

DNSSEC通过增加新的资源记录及相应的处理过程，完成对普通DNS消息中资源记录的认证。

A. 2.1 DNSSEC中增加的资源记录

为了实现DNSSEC，增加了如下资源记录。

A. 2.1.1 DNSKEY RR

DNSSEC 使用公钥算法来对 DNS 资源记录集签名和认证。私钥一般本地保存，不通过网络传送，用于对 DNS 资源记录集签名过程。公钥保存在 DNSKEY RR 中，用于 DNSSEC 认证过程。解析器通过公钥对签名进行认证。

DNSKEY RR 的类型值是48。

A. 2.1.1.1 DNSKEY RDATA格式

KEY RR的RDATA包含了标志，协议八位位组，算法数值八位位组，和公钥本身。格式如图A.1：

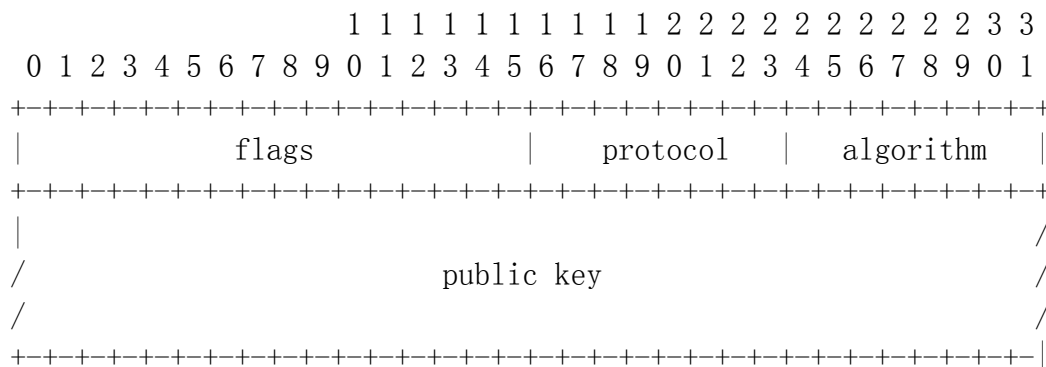


图 A. 1

A. 2.1.1.2 各字段定义

a) 标志位

比特0-6 和8-15都应该保留并且置0，在处理时应该忽略，比特7置1时，KEY RR中应该是区的公钥。当比特7为0时，KEY RR中保留的是其他类型的密钥。

b) 协议八位位组

协议八位位组应该置3，表示是应用于DNSSEC。

c) 密钥算法

该字段标识了公钥算法，“公钥”字段的格式随算法的不同而不同。

A. 2. 1. 1. 3 DNSKEY RR举例

下面为exmaple.com的DNSKEY RR。

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3
                                         Cbl+BBZH4b/0PY1kxkmvHjcZc8no
                                         kfzj3lGajIQKY+5CptLr3buXA10h
                                         WqTkF7H6RfoRqXQeogmMHfpftf6z
                                         Mv1LyBUGia7za6ZEzOJBOztyvhjL
                                         742iU/TpPSEDhm2SNKLiJfUppn1U
                                         aNvv4w== )
```

前面四个字段分别说明所有者名字，TTL，类别和RR类型（DNSKEY）。256说明“标签”字段的比特7的值为1，3是一个固定值，5说明了公钥算法，这里指的RSA/SHA1，其余为公钥的值。

A. 2. 1. 2 RRSIG RR

数字签名保存在 RRSIG RR 中，用于 DNSSEC 认证过程。支持 DNSSEC 的解析器能够根据这些 RRSIG RR 及公钥来对区中的资源记录集进行认证。

RRSIG RR 的类型值是46。

A. 2. 1. 2. 1 RRSIG RDATA 格式

RRSIG RR的RDATA部分如图A. 2所示：

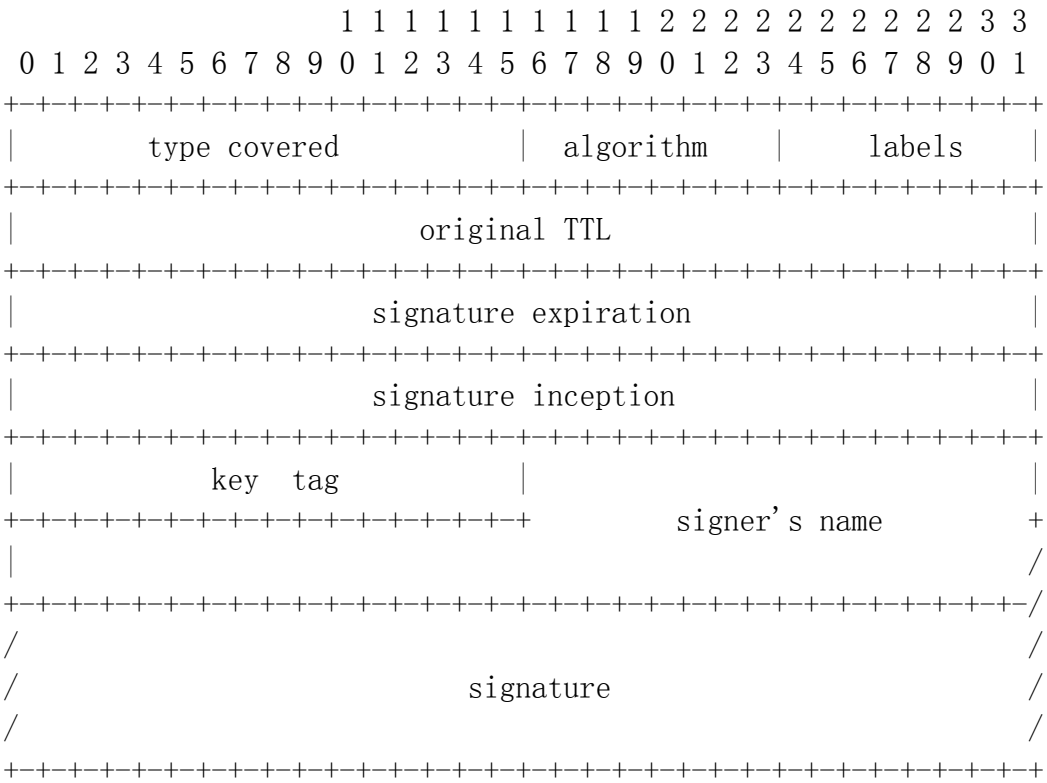


图 A. 2

A. 2. 1. 2. 2 各字段定义

a) 包含类型

该值必须和被签名的资源记录的类型相同。

b) 算法值

该字段的值标识了生成该签名的加密算法。

c) 标签数

“标签”八位位组是一个无符号值，表示初始RRSIG RR的所有者名字中包含的标签（label）数量。该字段可以使验证者能够判断出应答中所有者名字是否经过通配符合成，如果经过合成，通过该字段可以确定产生该签名的初始所有者名字。

d) 初始TTL

“初始TTL”包括在RDATA部分中，由于解析器会减少缓存的RRset的TTL值，而为了验证签名，解析器需要原来的RRSIG RDATA外的TTL值，因此需要保留该字段。初始TTL的值必须大于等于TTL的值。

e) 签名过期时间和起始时间

在“签名起始时间”到“签名过期时间”这段时间内，RRSIG都是有效的。二者都是从GMT 1970年1月1日开始到现在的无符号秒数，但不包括闰秒。

f) 密钥标记

“密钥标记”的值应该和用于认证签名的DNSKEY RR中的密钥标记值相同。

g) 签名者名字

签名者名字字段标识了解析器用来验证签名的DNSKEY RR的所有者名字。签名者名字必须包含签名RRset所属的区的名字。发送者在发送RRSIG RR时不能在签名者名字字段使用DNS名字压缩格式，而在接收者接收到包含压缩格式的签名者名字字段时应该能够解压缩该字段。

h) 签名

RRSIG RR 的签名字段是对 RRSIG RDATA(不包括签名字段本身)和由 RRSIG 的所有者名字，RRSIG 类别和 RRSIG 包含类型确定的 RRset 的签名。

应该按照下面的顺序生成资源记录的 RRSIG (这里“|”表示数据串联)

signature = sign(RRSIG_RDATA | RR(1) | RR(2)...)

RR(N) = name | class | type | TTL | RDATA length | RDATA

A. 2. 1. 2. 3 RRSIG RR举例

下面为host.example.com 某个RRset的RRSIG RR。

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 (
                                20030220173103 2642 example.com.
                                oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
                                PYGv07h108dUKGMeDPKi jVCHX3DDKdfb+v6o
                                B9wfuH3DTJXUAfI/M0zmO/zz8bW0Rzn1803t
                                GNazPwQKkRN20XPXV6nwwfoXmJQbsLNRlfkG
                                J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

前四个字段为所有者名字，TTL，类别和RR类型（RRSIG），A为包含类型，5说明产生签名所使用的算法（RSA/SHA1），3是初始所有者名字的标签个数，86400为所报告的A RRset的初始TTL，20030322173103和20030220173103为签名过期时间和起始时间，2642为密钥标签，example.com. 为签名者名字，其余为签名。注意，算法，签名者名字和密钥等几个字段说明这个签名可以通过example.com区的密钥标签为2642的密钥，通过算法5进行认证。

A. 2. 1. 3 NSEC RR

NSEC 资源记录包含了两部分内容：按照区名称顺序排列的下一个 RRset 的所有者名字，和该所有者的所有 RR 的类型的集合。全部的 NSEC RR 集合既指明了在一个区中存在哪些 RRset，同时也组成了所有者名字的链。该记录可以提供不存在的 DNS 数据类型。

NSEC RR的类型值为47。

A. 2. 1. 3. 1 NSEC RDATA格式

NSEC RR 的RDATA只包含一个域名，后面是一个比特图。如图A. 3所示：

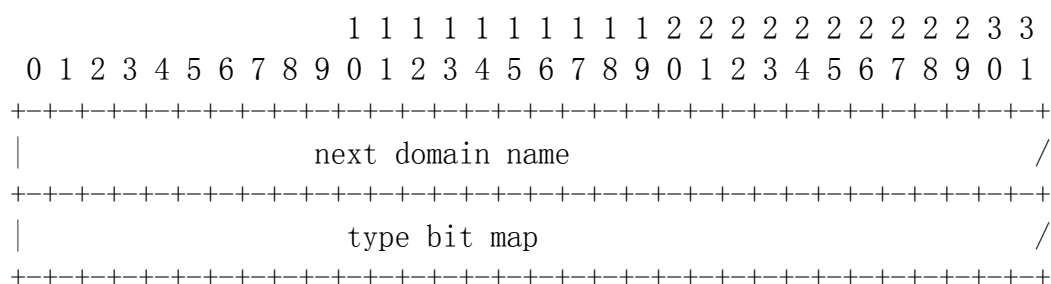


图 A. 3

“下一个域名字段”包含了区中按规范次序排列的下一个 RRset 的所有者名字。区中最后一个 NSEC 记录的“下一个域名字段”的值是区顶点的名字。

“类型比特图”字段标识了在 NSEC RR 的所有者名字中存在的 RRset 类型。该字段的每个比特都对应一个 RR 类型。比特 1 对应 RR 类型 1 (A)，比特 2 对于 RR 类型 2 (NS)，等等。如果某个比特置 1，则说明在对应 NSEC RR 的所有者名字中，该类型的 RRset 存在，反之，则不存在。

A. 2. 1. 4 DS RR

DS RR 指向一个 DNSKEY RR，用于 DNS DNSKEY 的认证过程。DS RR 存储了一个 DNSKEY RR 的密钥标签、算法和摘要。注意，虽然摘要足可以标识一个密钥，但是使用密钥标签和算法可以使认证过程效率更高。通过对 DS RR 的认证，解析器可以认证该 DS RR 指向的 DNSKEY RR。

DS RR 和相应的 DNSKEY RR 存储在不同的“区”文件中，DS RR 存储在 DNSKEY RR 授权“区”的父区。比如，区“example.com”的 DS RR 存储在“com”区（父区）中，而不是存储在“example.com”中，而相应的 DNSKEY RR 存储在“example.com”（子区）中。

DS RR 的类型值为 43。

A. 2. 1. 4. 1 DS RDATA 格式

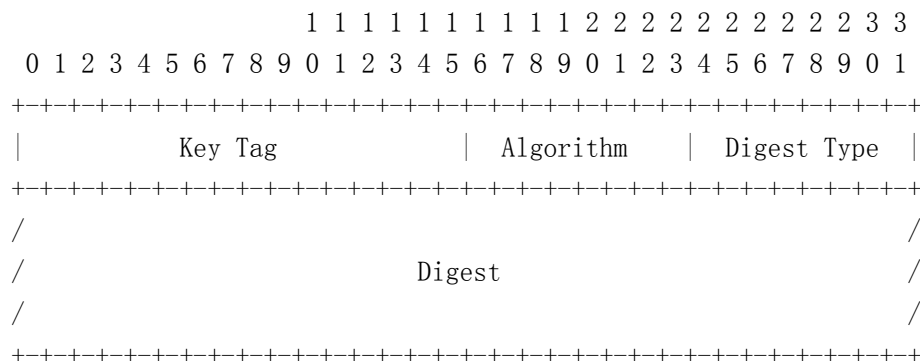


图 A. 4

A. 2. 1. 4. 2 DS RDATA 各字段定义

- 密钥标签字段标识了 DS 记录指向的 DNSKEY RR 中的密钥标签。DS RR 中的该字段值应该同 RRSIG RR 中的该字段值相等。
- 算法字段标识了由 DS RR 指向的 DNSKEY RR 的算法值。DS RR 中的该字段值和 RRSIG 及 DNSKEY RR 中该字段值相等。
- 摘要类型字段：DS RR 通过包括 DNSKEY RR 的摘要指向 DNSKEY RR。摘要类型字段标识了生成该摘要的算法。
- 摘要字段：DS RR 通过包括 DNSKEY RR 的摘要指向 DNSKEY RR。摘要字段包含了该摘要。该摘要的计算方法如下：

digest = digest_algorithm(DNSKEY 所有者名字 | DNSKEY RDATA)

“|” 标识串联

DNSKEY RDATA = Flags | Protocol | Algorithm | Public Key

A.2.1.4.3 DS RR举例

下面给出一个DNSKEY RR和相应的DS RR。

```
dskey.example.com. 86400 IN DNSKEY 256 3 5 ( AQOeiiR0GOMYkDshWoSKz9Xz
fwJr1AYtsmx3TGkJaNXVbfi/
2pHm822aJ5iI9BMzNXxeYcmZ
DRD99WYwYqUSdjMmmAphXdvx
egXd/M5+X7OrzKBaMbCVdFLU
Uh6DhweJBjEVv5f2wwjM9Xzc
nOf+EPbtG9DMBmADjFDc2w/r
ljwvFw==
) ; key id = 60485

dskey.example.com. 86400 IN DS 60485 5 1 ( 2BB183AF5F22588179A53B0A
98631FAD1A292118 )
```

前四个字段指定了姓名, TTL, Class, 和RR类型 (DS), 60485是和 “dskey.example.com.”DNSKEY RR 相对应的密钥标签, 5说明和 “dskey.example.com.” DNSKEY RR 相对应的是算法5, 1说明产生摘要的算法, 其余为摘要值。

A.2.2 DNSSEC对服务器的要求

具有安全性的服务器必须支持EDNS0[RFC2671]消息。

A.2.2.1 授权名字服务器

当收到的请求的EDNS[RFC2671]OPT pseudo-RR DO比特[RFC3225]置1时, 支持DNSSEC的名字服务器必须根据特定规则在应答中包括RRSIG RR, NSEC RR, DS RR等等。详细描述请参考[RFC 4035]。

A.2.2.2 递归名字服务器

支持DNSSEC的递归名字服务器同时具有名字服务器和解析器的功能。本节中使用“名字服务部分”和“解析器部分”来分别指定在支持DNSSEC的递归名字服务器中实现名字服务器功能的部分和实现解析器功能的部分。

A.2.2.2.1 DO比特

支持DNSSEC的递归名字服务器的“解析器部分”在发送请求时必须将DO比特置位, 而不论从“名字服务器部分”收到的DO比特如何。

A.2.2.2.2 CD比特

CD 比特可以使解析器通知支持 DNSSEC 的名字服务器: 在处理一个特定请求的过程中, 禁止进行签名验证。

具有安全性的递归服务器必须忽略CD, 来执行正常的签名验证, 除非:

- “名字服务器部分”通过安全通道收到请求;
- 递归服务器的本地策略认为CD比特优先级更高, 即使通过不安全的通道收到数据。

A.2.2.2.3 AD比特

除非当支持DNSSEC的名字服务器的“名字服务器部分”认为应答中的answer或者authority部分的所有RRset都是可信的, 否则“名字服务器部分”决不能在应答中设置AD比特, 并且当且仅当“解析器部分”认为answer部分和在authority部分中的否定应答的RR都是经过认证的, “名字服务器部分”才应当将AD比特置位。

A.2.3 DNSSEC应答中RR的认证过程

为了使用 DNSSEC RR 来认证, 解析器需要预先配置至少一个已经认证的 DNSKEY 或者 DS RR。获得和认证该初始的 DNSKEY 或者 DS RR 需要通过外部的机制。以下过程假设解析器已经获得初始的认证 DNSKEY RR。

初始DNSKEY RR可以被用来认证一个区的顶点DNSKEY RRset。为了使用初始密钥来认证顶点DNSKEY RRset，解析器必须能够：

- 验证初始的DNSKEY RR出现在顶点DNSKEY RRset，并且验证DNSKEY RR的区密钥标志 (DNSKEY RDATA的比特7) 为1。
- 证明存在RRSIG RR对顶点的DNSKEY RRset签名，使用RRSIG RR和初始DNSKEY RR共同来认证DNSKEY RRset。

一旦解析器使用一个初始DNSKEY RR认证了顶点DNSKEY RRset，通过该区的DS RR就可以认证该区的授权子区了。这使得解析器从一个初始密钥开始，然后使用DS RRset，层层递归到DNS树底，来获得其他区的顶点DNSKEY RRset。如果解析器配置了根DNSKEY RR，并且从根开始，每个授权子区都有一个相关的DS RR，则解析器能够获得和验证所有区的顶点DNSKEY RRset。

一旦解析器认证一个区的顶点DNSKEY RRset，下面需要认证两部分内容：1. 解析器使用顶点DNSKEY RRset中的DNSKEY RR和该区的RRSIG RR来认证该区中的任意RRset；2. 解析器通过认证的区中的NSEC RRset来证明在区中不存在的RRset。

A. 2. 3. 1 认证DNSKEY RR

一旦一个区的父区的顶点DNSKEY RRset通过认证，则该父区的DS RR可以用来认证子区。DS RR标识了子区的顶点DNSKEY RRset中的DNSKEY RR，并且包含了子区的DNSKEY RR的加密摘要。加密摘要算法可以保证攻击者很难根据摘要产生DNSKEY RR。这样，解析器对摘要的认证相当于对DNSKEY RR的认证。解析器可以使用这个子区的DNSKEY RR来认证子区顶点全部的DNSKEY RRset。假设已经得到子区的DS RR，如果下列条件满足，子区的顶点DNSKEY RRset可以被认证。

- 通过父区的顶点DNSKEY RRset中的某个或某些DNSKEY RR，父区的DS RR已经通过认证。
- DS RR的算法和密钥标签和子区的顶点DNSKEY RRset中的DNSKEY RR的算法和密钥标签匹配，该DNSKEY RR通过使用DS RR中的“摘要类型”的hash算法，产生的摘要值和DS RR中“摘要”字段内容相同。
- 子区中匹配的DNSKEY RR的“区标志”比特置为1，说明相应的私钥已经对子区的顶点DNSKEY RRset签名，产生的RRSIG RR可以认证子区的顶点DNSKEY RRset。

A. 2. 3. 2 通过RRSIG RR认证RRset

解析器可以使用RRSIG RR和相应的DNSKEY RR来认证RRset。该过程可以分成三步：

- 解析器先检验RRSIG RR是否覆盖了RRset，是否有一个有效的时间间隔，是否标识了一个有效的DNSKEY RR。
- 解析器在签名的RRset后添加RRSIG RDATA(不包括签名字段)组成签名数据的规范形式。
- 最后，解析器使用公钥和签名来认证签名数据。

A. 2. 3. 3 认证不存在数据

解析器可以使用认证的NSEC RR来证明在一个签名区里不存在某个RRset。支持DNSSEC的服务器应该在给支持DNSSEC的应答中自动包含必要的NSEC RR。

安全解析器必须根据上一节RRset的认证规则首先来认证NSEC RRset，然后：

- 如果请求的RR名字和经过认证的NSEC RR的所有者名字匹配，则NSEC RR的“类型比特图”列举了所有者名字中所有存在的RR类型，解析器可以通过检查“比特图”中的RR类型来证明请求的RR类型不存在。
- 如果按照规范的DNS名字次序，请求的RR名字在经过认证的NSEC RR所有者名字后，而在NSEC RR的“下一个域名字段”列举的名字前，则在区中没有请求的RR名字。

A. 2. 3. 4 认证过程举例

以下是对应答中RR验证的一个可能的例子，假设应答如下：

```
;; Header: QR AA DO RCODE=0
;;
```

;; Question

x.w.example. IN MX

;; Answer

x.w.example. 3600 IN MX 1 xx.example.

```
x.w.example. 3600 RRSIG MX 5 3 3600 20040509183619 (
20040409183619 38519 example.
I12WTZ+Bkv+OytBx4LItnNW5mjB4RCwh008y1
XzPHZmZUTVYL7LaA63f6T9ysVBzJRI3KRjAP
H3U1qaYnDoN1DrWqmi9RJe4FoObkbcdm7P3I
kx70ePCoFgRz1Yq+bVVXCvGuAU4xALv3W/Y1
jNSlwZ2mSWKHfxFQxPtLj8s32+k= )
```

;; Authority

example. 3600 NS ns1.example.

example. 3600 NS ns2.example.

```
example. 3600 RRSIG NS 5 1 3600 20040509183619 (
20040409183619 38519 example.
g1l3F00f2U0R+SWiXXLHwsMY+qStYy5k6zfd
EuivWc+wdlfmbNCyql0Tk7lHTX6UOxc8AgNf
4ISFve8XqF4q+o9qlnqIzmppU3LiNeKT4FZ8
RO5urFOvoMRTbQxW3U0hXWugge4g3ZpsHv48
0HjMeRaZB/FRPGfJPa jngcq6Kwg= )
```

;; Additional

xx.example. 3600 IN A 192.0.2.10

```
xx.example. 3600 RRSIG A 5 2 3600 20040509183619 (
20040409183619 38519 example.
kBF4YxMGWF0D8r0cztL+2fWWOvN1U/GYSpYP
7SoKoNQ4fZKyK+weWGlKLIUM+uE1zjVTPXoa
0Z6WG0oZp46rkl1EzMcdMgoaeUzzAJ2BMq+Y
VdxG9IKlyZkYGY9AgbTOGPoAgbJyO9EPULsx
kbIDV6GPPSZVusnZU6OMgdgzHV4= )
```

xx.example. 3600 AAAA 2001:db8::f00:baaa

```
xx.example. 3600 RRSIG AAAA 5 2 3600 20040509183619 (
20040409183619 38519 example.
Zzj0yodDxcBLnnOIwDsuKo5WqiaK24DlKg9C
aGaxDFiKgKobUj2jilyQHpGFn2poFRetZd4z
ulyQkssz2QHrVrPuTMS22knudCiwP4LWpVTr
U4zfeA+rDz9stmSBP/4PekH/x2IoAYnwctd/
xS9cL2QgW7FChw16mzlkH6/vsfs= )
```

ns1.example. 3600 IN A 192.0.2.1

```
ns1.example. 3600 RRSIG A 5 2 3600 20040509183619 (
20040409183619 38519 example.
```

```

F1C9HVhIcs10cZU09G5yIVfKJy5yRQQ3qVet
5pGhp82pzhAOMZ3K22JnmK4c+IjUeFp/to06
im5FVpHtbFisdjyPq84bhTv8vrXt5AB1wNB+
+iAqvIfdgW4sFNC6oADb1hK8QNauw9VePJhK
v/iVXSYC0b7mPSU+E0lknFpVECs= )
ns2.example. 3600 IN A 192.0.2.2
ns2.example. 3600 RRSIG A 5 2 3600 20040509183619 (
20040409183619 38519 example.
V7cQRwlTR+knlaL1z/psxlS1PcD37JJDaCMq
Qo6/ulqFQu6x+wuDHRH22Ap9ulJPQjFwMKOu
yfPGQPC8KzGdE3vt5snFEAoElVn3mQqtu7SO
6amIjk13Kj/jyJ4nGmdRIc/3cM3ipXFhNTKq
rdhx8SZ0yy40bIRzIzvBFLiSS8o= )

```

服务器在应答中返回域“x.w.example.com”的 MX RRset，相应的 RRSIG 说明 MX RRset 由“example”DNSKEY 的密钥标签为 38519，算法为 5 来签名。解析器需要相应的 DNSKEY RR 来认证该应答。下面来讨论解析器可能获得的 DNSKEY RR 的方法。

假设解析器已经配置一个“根”的 DNSKEY RR（或者配置了“根”的 DS RR），解析器检查该配置的 DNSKEY RR 是否在根的 DNSKEY RRset 中（或者 DS RR 是否和根的 DNSKEY RRset 中的某个 DNSKEY 匹配），该 DNSKEY RR 是否已经对“根”的 DNSKEY RRset 签名，且签名在有效期内。如果所有这些条件都满足，则所有在 DNSKEY RRset 中的密钥都是经过认证的。解析器可以使用一个（或多个）“根”的 DNSKEY RR 来认证“example”的 DS RRset。注意解析器可能需要向“根”区发送请求来获得“根”的 DNSKEY RRset 和/或“example”的 DS RRset。

一旦通过“根”DNSKEY 认证的“example”的 DS RRset，解析器检查“example”DNSKEY RRset，来寻找某个“example”DNSKEY RR 和已认证的“example”DS RR 相匹配。如果找到匹配的“example”DNSKEY，解析器检查该 DNSKEY RR 是否已经对“example”DNSKEY RRset 签名并且签名在有效期内。如果条件满足，则所有在“example”DNSKEY RRset 中的密钥都认为是通过认证的。

最后，解析器使用算法 5 和密钥标签 38519。该 DNSKEY 用来认证包含在应答中的 RRSIG。如果多个“example”DNSKEY 都是算法 1 和密钥标签为 5742，则每个 DNSKEY RR 都要认证一次，并且只有当每个 DNSKEY RR 都能认证该签名时，该应答中的 RRSIG 才可以通过认证。

附 录 B

(资料性附录)

TSIG 和 SIG (0)

除了DNSSEC外，还可以通过增加另外两种资源记录(TSIG和SIG(0))实现对DNS请求和应答的交互过程的认证。

B.1 TSIG

TSIG提供了通过共享密钥和散列算法来进行交互认证的一种方法。接收者通过对接收到的在原有DNS消息上添加的TSIG记录的验证，能够完成对发送者发送的消息的验证。

以下是对TSIG的简单描述，详细过程按照RFC 2845的规定。

B.1.1 TSIG格式

```

NAME
TYPE
CLASS
TTL
RdLen
RDATA
    Algorithm Name
    Time Signed
    Fudge
    MAC Size
    MAC
    Original ID
    Error
    Other Len
    Other
  
```

其中，消息验证码(MAC)放在MAC之中，其他字段请见[RFC2845]。

B.1.2 TSIG计算

目前唯一定义的摘要算法是”HMAC-MD5” [RFC1321], [RFC2104]。

B.1.2.1 TSIG的处理

a) 发送消息中添加TSIG的影响

在组成发送的消息时，应该计算带密钥的消息摘要。生成的消息摘要保存在TSIG中，添加在附加数据段中(ARCOUNT也要增加)。如果TSIG记录增加后会引起消息过长而要分开发送，服务器必须变换该应答使TSIG能够包含进去。变换后的应答只包含问题和TSIG记录，且TC比特置位，RCODE=0(NOERROR)。

b) 在接收消息中TSIG的处理

如果接收到的消息包含TSIG记录，则TSIG必须是附加段中的最后一个记录。不允许出现多个TSIG记录。如果TSIG记录出现在其他位置，该包可以丢弃，同时回送RCODE=1(FORMERR)。如果收到一个位置正确的TSIG RR，则从DNS消息中取出TSIG，并减少DNS消息头中的ARCOUNT。之后进行带密钥的消息摘要的验证。如果算法名或者密钥名不可知，或者消息摘要不匹配，则DNS消息应该拒绝。如果该消息是请求消息，应答中的RCODE必须等于9(NOTAUTH)，TSIG ERROR=17(BADKEY)或者TSIG ERROR=16(BADSIG)。如果没有密钥对该消息加密，则MAC size== 0并且MAC为空。

B.2 SIG(0)

SIG(0)通过对DNS请求和/或应答的交互的签名,提供了另一种对交互认证的方法。因为该SIG记录的覆盖类型=0, 因为被称作SIG(0)。

以下是对SIG(0)的简单描述, 详细过程请参考[RFC2931]。

B.2.1 SIG(0)资源记录

对于所有的交互SIG(0), 签名者字段必须是初始的主机名, 且该主机必须拥有和签名的私钥相对应的公钥。

对于所有的SIG(0) RR, 所有者名字, 类别, TTL和初始TTL都是没有意义的。TTL字段应该等于0, 类别字段应该是ANY。为了节省空间, 所有者名字字段应该是根(值为0的八位位组)。但需要对应答进行SIG(0)认证时, 在应答中包含的附加信息中, SIG RR的优先级必须最高。如果由于包含SIG(0), 而使得消息被分开发送, 服务器必须变换该消息使得能够包含SIG(0)。变换后的应答只包含问题和SIG资源记录, 且TC比特置位, RCODE=0(NOERROR)。此时客户端应该通过TCP重新发送请求。

B.2.2 SIG(0)处理

B.2.2.1 计算请求和交互SIG

DNS请求可以通过在请求的“附加信息段”的尾部包含一个SIG(0)来签名。该SIG由“覆盖类型”字段=0标识。它对该消息前面的DNS请求签名, 包括DNS头, 但是不包含UDP/IP头, 因为包含了请求SIG(0), RR数量也应该调整。

SIG(0)通过下面两个部分的数据来计算(1)除了RDATA段中的签名字段不包括(而不是将签名字段置0)外, 包括SIG RDATA的全部字段(2)DNS请求消息, 包含DNS头, 但是不包含UDP/IP头, 并且RR数量因为包含了请求SIG(0)也应该调整。即:

$$\text{data} = \text{RDATA} \mid \text{request} - \text{SIG}(0)$$

这里“|”是串联, RDATA是SIG(0)的RDATA, 但不包括签名本身。

相似的, SIG(0)可以用来对请求和应答的交互进行签名。该交互签名通过以下数据来计算(1)除了签名部分的SIG RDATA(2)全部的DNS请求消息, 包括请求的DNS头, 但不包括UDP/IP头(3)DNS应答消息, 包括DNS头, 但不包括UDP/IP头, 并且RR数量因为包含了请求SIG(0)也应该调整。即:

$$\text{data} = \text{RDATA} \mid \text{full query} \mid \text{response} - \text{SIG}(0)$$

解析器对应答SIG(0)的验证可以说明请求和应答在传递过程中没有被篡改, 应答和请求是对应的, 并且应答来自于请求的服务器。

注意: 请求和应答可以包括一个TSIG或者SIG(0), 但是不能同时包括TSIG和SIG(0)。

B.2.2.2 处理应答和SIG(0) RR

如果SIG RR在附加信息段的尾部, 并且“覆盖类型”=0, 则这是一个包含应答和响应的事务交互签名。如果应答的SIG(0)检查通过, 该交互认证SIG不能直接证明消息中任何数据RR的正确性。因为产生SIG(0)的私钥是属于某个主机的, 而对资源记录签名的私钥是属于某个区的。然而, 它证明了该应答由请求的服务器发出, 并且没有篡改。若解析器或者服务器没有实现交互和/或请求SIG, 则当这是可选时, 解析器或服务器必须忽略SIG(0)而不应该产生错误; 当是必选时, 应该认为失败。

附 录 C (资料性附录)

采用 EPP 协议提供和管理 E. 164 号码的技术要求

EPP 是可承载于多种传输层协议之上的有状态的 XML 协议。通过使用低层安全协议进行保护，客户端与服务器交换身份标识、鉴权和选项信息，并进行一系列由客户端发起的命令—响应交互。所有 EPP 操作都是原子的（不可分为多个子操作执行），这使得它们都是幂等的（多次执行一个操作等效于执行一次该操作）。

EPP 提供四种基本服务元素：业务发现、命令、响应和扩展框架，该框架支持对被管理对象进行定义，并定义了这些对象的协议请求与响应之间的关系。

EPP 服务器必须为客户端发起的通信（可能是低层连接请求或 EPP 业务发现消息）返回 greeting 作为响应。服务器必须为每个 EPP 命令迅速做出响应。图 C. 1 为服务器状态机，描述了消息交互处理细节。

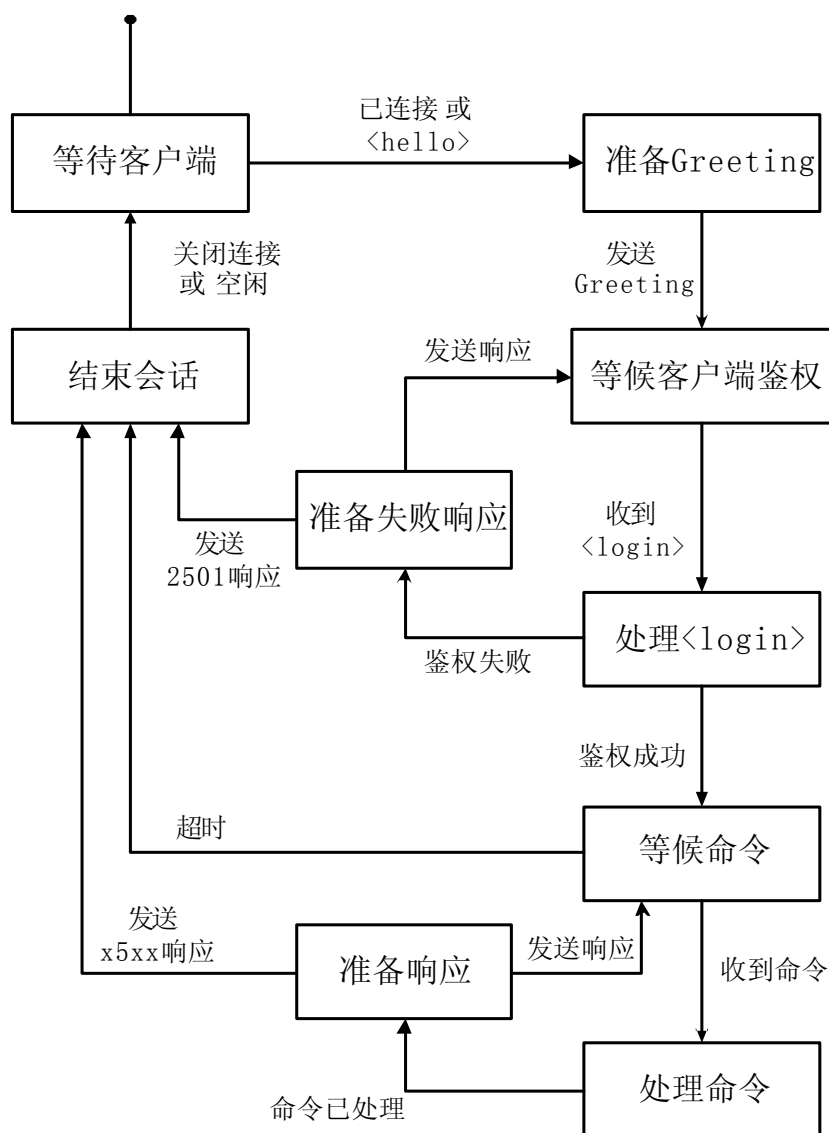


图 C. 1 EPP 协议服务器状态机

EPP 命令分为 3 类：会话管理命令、查询命令、数据更改命令。会话管理命令用于建立和结束与

EPP 服务器保持的会话。查询命令用于执行对象信息获取只读操作。更改命令拥护执行对象管理读写操作。

服务器按照从客户端接收的顺序处理命令。服务器可以立即做出响应确认对命令的接收和处理。此外，协议还提供了在请求动作完成之前允许脱机复查更改命令的功能。在这种情况下，服务器的响应必须清楚地说明这个命令已被接收并处理，但请求操作未决。相应对象的状态应当清楚地反映正在处理未决操作。当该操作脱机处理完成后，服务器必须通知客户端。对象映射应当描述表示脱机处理完成的通告的标准格式。

EPP 使用 XML 名字空间(namespace)提供扩展对象管理框架，并标识 XML 实例解析和确认所需的模式(schema)。名字空间和模式定义用于标识基本协议模式和用于被管理对象的模式。

利用EPP提供的扩展规则，可将协议操作映射至特定对象，在协议原有基础上为对象添加新的功能，达到对协议扩展的目的。使用EPP实现提供和管理存储在共享中心数据库中因特网域的机制称为EPP域名映射(EPP Domain Mapping)。该映射使用XML语言定义应用于域名的EPP命令语法和语义。EPP E. 164号码映射是对EPP域名映射的扩展，在域名映射的基础上添加了有关E. 164号码相关的内容，该映射使用XML语言定义应用于E. 164号码的EPP命令语法和语义。

C.1 协议标识

所有EPP XML实例，必须以<epp>开始，以</epp>结束。该元素可以标识协议所在名字空间(namespace)，以及协议模式的位置(location of protocol schema)。

C.2 对象标识

全球唯一标识符(GUID)有助于在共享数据库之间使用对象信息。在对象创建时，必须为其分配一个全球唯一标识。该标识符必须作为每个请求的一部分返回给客户端，用于获取对象的详细属性。

C.3 对象属性

一个EPP域对象具有属性及与其关联的值，可以通过赞助商客户端或服务器进行查看或修改。

C.3.1 域和主机名(Domain and Host Names)

一个服务器可将允许使用的域名限定为某个顶级域、二级域或该服务器拥有授权的其他域。域名末尾的点(".")必须隐含包括在DNS区域中，在主机和域名交互过程中不得使用。

C.3.2 联络和客户标识符(Contact and Client Identifiers)

一个服务器唯一标识符标识了所有的EPP联络方式。联络标识符具有最小和最大字符串长度限制，以及指定的格式。联络标识符使用EPP协议中定义的"clIDType"客户端标识符语法。

C.3.3 状态值(Status Values)

一个域对象至少有一个关联的状态值。只有域对象赞助商的客户端和对象所在主机可以设置该对象的状态值。用户可以使用 EPP<update>命令改变域对象的状态。每个状态值可附带可读的文本，用于描述应用对象状态的理由。

用户不能改变服务器设定的状态值。服务器可以更改或覆盖客户对象根据本地服务器策略设定的状态值。对象状态可能由于服务器发起的更改命令或服务器管理员的操作发生改变。

"client"前缀表示客户端可添加或删除的状态。"server"前缀表示服务器可添加或删除的状态。不采用以上两种前缀的状态为服务器管理状态。已定义的状态值如下：

- clientDeleteProhibited, serverDeleteProhibited
- clientHold, serverHold
- clientRenewProhibited, serverRenewProhibited
- clientTransferProhibited, serverTransferProhibited
- clientUpdateProhibited, serverUpdateProhibited

- inactive
- ok
- pendingCreate, pendingDelete, pendingRenew, pendingTransfer, pendingUpdate

C.3.4 日期与时间(Date and Time)

日期和时间属性值必须使用公历的全球统一时间(UTC)表示。必须使用大写“T”和“Z”定义的扩展date-time格式表示date-time值,因为XML模式不支持删节的data-time格式,以及小写的“t”和“z”。

C.3.5 有效期(Validity Periods)

如果服务器策略支持域名对象的有效期,当创建域名对象的时候为其定义有效期,有效期可能通过EPP<renew>或<transfer>命令进行延长。本规范未定义超出域名对象服务有效期后需要进行的操作。它将由服务器策略自己决定。

有效期可以按年或月计量,使用“unit”属性来区分。“y”表示年,“m”表示月。最小的数值为1,最大的数值为99。服务器可支持最大值下限。

C.3.6 鉴权信息(Authentication Information)

鉴权信息与域对象关联,用于转让操作。鉴权信息是在域对象创建的时候建立的,它可能会在以后被更新。本规范描述了基于密码的鉴权信息,还可使用其他机制。

C.3.7 其他DNS资源记录属性

当DNS允许多种资源记录类型与域关联时,该映射仅被用于显式地指定那些描述用于域授权和解析资源记录的元素。可通过扩展此映射开发提供其他域相关资源记录类型的工具。

C.3.8 E.164域名

E.164域名用来表示一个E.164号码,该E.164号码的翻译遵循域名语法,在ENUM规范(RFC 3761)中对此进行了描述。

C.3.9 NAPTR 字段(Field)

根据 ENUM 规范,命名授权指针(NAPTR)资源记录用于标识与指定节点联系的可用方式,该节点是由从一个 E.164 号码翻译创建的域名标识的。

NAPTR字段包括以下部分:

- Order, 16位无符号整数, unsignedShort”类型。
- Preference, 16位无符号整数, unsignedShort”类型
- Flags, 单个字符, 不区分大小写。
- Service, 最大长度为65个字符的字符串。
- regexp (Regular Expression), 无长度限制的字符串。
- Replacement, 最大长度为255的字符串。

C.4 EPP业务连接的建立

EPP 可承载于面向连接或面向非连接的传输协议之上。一个 EPP 客户可随时通过发送一个<hello>给服务器,向它请求<greeting>。对于客户的请求,服务器要返回带有<greeting>的响应。

<hello>必须为不带有子元素的空元素。

<greeting>元素包含以下元素:

- 一个<svID>元素。
- 一个<svDate>元素。
- 一个<svcMenu>元素,它包含以下子元素:
 - 一个或多个<version>元素。
 - 一个或多个<lang>元素。
 - 一个或多个<objURI>元素。
 - 一个<svcExtension>元素(可选)。

- 一个<dcP>元素包含以下子元素：
 - a) 一个<access>元素包含下列元素之一：<all/>、<none/>、<null/>、<personal/>、<personalAndOther/>、<other/>。
 - b) 一个或多个<statement>元素必须包含下列所有元素：<purpose>、<recipient>、<retention>。其中<purpose>必须包含下列一个或多个元素：<admin/>、<contact/>、<prov/>、<other/>;<recipient>必须包含下列一个或多个元素：<other/>、<ours>（包含可选的<recDesc>）、<public/>、<same/>、<unrelated/>;<retention>必须包含下列元素之一：<business/>、<indefinite/>、<legal/>、<none/>、<stated/>。

——一个<expiry>元素（可选），必须包含下列子元素之一：

- <absolute/>。
- <relative/>。

C.5 E.164 相关EPP命令

C.5.1 通用EPP命令格式

EPP命令基于请求—响应机制。EPP命令包含都是由客户端发往服务器的请求(request)和服务器返回给客户端的响应(response)。

C.5.1.1 请求命令格式：

EPP客户端发送命令给EPP服务器，并接收从服务器返回的响应。除标准的EPP元素之外，EPP命令还包含下列元素：

- 命令标签，可以是协议相关的也可以是对象相关的。
- 一个<extension>元素（可选），指定服务器定义的命令扩展。
- 一个<clTRID>元素（可选），transaction ID，客户端维护的交易标识。

C.5.1.2 响应命令格式：

EPP服务器对客户端发起的命令回以响应。EPP响应包含以下元素：

——一个或多个<result>元素。每个<result>元素包含以下内容：

- 一个“code”属性，4位10进制数，描述命令的成功或失败。
- 一个<msg>元素，包含可读的响应代码描述。
- 零个或多个<value>（可选），指示客户所提供的导致服务器错误状态的值。
- 零个或多个<extValue>（可选），用于提供额外的诊断信息，包含以下元素：
 - a) 一个<value>元素。
 - b) 一个<reson>元素。

——一个<msgQ>元素（可选），描述消息进入队列，等待客户端获取。包含以下属性：一个“count”属性和一个“id”属性。

<msgQ>元素包含以下可选的子元素：

- 一个<qDate>元素，描述消息入队的日期和时间。
- 一个<msg>元素，包含可读信息。

——一个<resDate>元素（可选）。

——一个<extension>元素（可选）。

——一个<trID>元素，服务器分配的事务号。

C.5.2 E.164号码相关EPP命令格式

E.164号码相关EPP命令有三种类型：会话管理命令，查询命令，数据更改命令。会话管理命令用于与EPP服务器建立和保持会话；查询命令用于获取只读对象信息；更改命令用于对可读写对象进行管理操作。

C.5.2.1 会话管理命令(Session Management Command)

C.5.2.1.1 <login>命令

<login>命令用于建立与 EPP 服务器间的会话，以响应服务器发起的问候(greeting)。<login>命令必须在其他命令之前发送给服务器，以建立一个会话。服务器管理员可能会限制登录失败尝试的次数 N ， $1 \leq N \leq \infty$ ，超过登录失败次数限制之后，到服务器的连接将被断开。

客户端标识和初始密码必须由服务器创建，在此之后客户端可以成功完成<login>命令。客户端标识和初始密码必须使用带外传输的方式发送给客户端，用来保护标识和密码不被泄露。

C.5.2.1.2 <logout>命令

<logout>命令用于结束与服务器间的会话。<logout>命令必须是不带任何子元素的空元素。服务器可能因为客户端长时间无操作或超出客户端会话期限而结束一个会话。

C.5.2.1.3 查询命令

EPP提供四种供查询对象信息的命令：<check>用于检查数据库中是否提供某个对象，<info>用于检索已知对象的关联信息，<poll>用户获取服务器上的通知消息，<transfer>用于获取对象转让状态信息。

C.5.2.1.4 <check>命令

除标准 EPP 命令元素外，<check>命令必须包含一个<domain:check>元素，标识域名字空间和域模式的位置。当命令成功处理后，返回的消息中<resData>元素必须包含<domain:chkData>元素，用于标识域名字空间和域模式位置。<domain:chkData>元素包含一个或多个<domain:cd>元素，该元素包含以下子元素：

请求命令包含下列元素：

——一个<domain:name>元素。

响应命令包含下列元素：

——一个<domain:name>元素。

——一个<domain:reason>元素(可选)。

<check>命令必须对所有已授权的客户开放。[EPP]

C.5.2.1.5 <info>命令

对于此获取信息的请求，服务器可以根据策略返回不同的信息；如果是赞助商客户端发起的请求，必须返回所有可用的信息；如果发起查询的客户不是赞助商客户端，但客户提供有效的授权信息，也必须返回所有可用信息；如果查询的客户不是赞助商客户端，且客户未提供有效的授权信息，服务器策略可以决定返回何种可选元素。

除标准的EPP命令元素外，<info>请求命令必须包含一个<domain:info>元素，标识名字空间和域模式的位置。<domain:info>包含以下子元素：

——一个<domain:name>。

——一个<domain:autoInfo>(可选)。

<info>命令成功处理后，返回响应中EPP<resData>必须包含<domain:infData>元素。必须返回所有非可选的元素；可根据客户授权情况和服务器策略决定需要返回的可选元素。<domain:infData>元素包含以下子元素：

——一个<domain:name>元素。

——一个<domain:roid>元素。

——零个或多个<domain:status>元素(可选)。

——一个<domain:registrant>元素(可选)。

——一个<domain:ns>元素(可选)。

——零个或多个<domain:host>元素(可选)。

——一个<domain:clID>元素。

——一个<domain:crID>元素(可选)。

——一个<domain:crDate>元素(可选)。

- 一个<domain:exDate>元素（可选）。
- 一个<domain:upID>元素（可选）。
- 一个<domain:upDate>元素（可选）。
- 一个<domain:trDate>元素（可选）。
- 一个<domain:authInfo>元素（可选）。

返回响应中要包含EPP<extension>元素，该元素必须包含<e164:infData>元素，用于标识e164名字空间和e164策略位置。<e164:infData>元素包含一个或多个<e164:naptr>元素，该元素包含下列子元素：

- 一个<e164:order>元素，包含一个NAPTR order值。
- 一个<e164:pref>元素，包含一个NAPTR preference值。
- 一个<e164:flags>元素，包含一个NAPTR flag值（可选）。
- 一个<e164:svc>元素，包含一个NAPTR service值。
- 一个<e164:regex>元素，包含一个NAPTR regexp值（可选）。
- 一个<e164:replacement>元素，包含一个NAPTR replacement值（可选）。

<info>命令应当限定给已授权的用户使用；建议限制此操作给赞助客户使用。[EPP]

C.5.2.1.6 <poll>命令

<poll>命令用于发现和获取服务器为单独的客户端安排的服务队列消息。如果消息队列不为空，则对<poll>命令的成功响应必须返回队列中第一条消息。服务器返回的每个响应包含服务器唯一消息标识符和指示消息队列中消息数目的数值。必须提供该标识符用于确认消息的接收。客户端收到消息后，必须使用明确的响应命令确认已经收到该消息。在收到客户端的接收确认后，服务器必须将消息退队，并减小队列长度值，使得下一条消息入队等待接收（如果有的话）。

<poll>命令必须为空元素，不带有子元素。

接收到的服务器消息队列的第一条消息，要求"op"属性值为"req"。

接收消息的确认响应，要求"op"属性值"ack"，"msgID"属性值为被确认消息中<msg>元素所对应的"id"值。

<poll>操作应限定给已授权的用户使用；建议消息入队和限制队列访问采取每客户机制。

C.5.2.1.7 <transfer>查询命令

作为查询的<transfer>命令必须带有值为"query"的"op"属性，此映射增加了<domain:transfer>元素。<domain:transfer>元素包含以下子元素：

- 一个<domain:name>元素。
- 一个<domain:authInfo>元素（可选）。

<transfer>响应命令的<resData>中必须包含一个<domain:trnData>元素，该元素包含下列子元素：

- 一个<domain:name>元素。
- 一个<domain:trStatus>元素。
- 一个<domain:reID>元素。
- 一个<domain:reDate>元素。
- 一个<domain:acID>元素。
- 一个<domain:acDate>元素。
- 一个<domain:exDate>元素（可选）。

<transfer>查询命令应当限定给已授权的用户使用；建议对请求和响应客户端进行查询限制。对象转让可能由于对象相关策略不可用或受限。

C.5.2.2 更改命令

E. 164 EPP命令有以下5种命令：<create>用于在服务器上创建对象实例，<delete>用于从服务器上删除对象实例，<renew>用于延长对象的有效期，<update>用于更改对象关联信息，<transfer>用于管理域对象的赞助商变更。

C. 5. 2. 2. 1 <create>命令

除标准EPP命令元素外，<create>请求命令必须包含一个<domain:create>元素，标识域名字空间和域模式的位置。该元素包含以下子元素：

- 一个<domain:name>元素。
- 一个<domain:period>元素（可选）。
- 一个<domain:ns>元素（可选）。
- 一个<domain:registrant>元素（可选）。
- 零个或多个<domain:contact>元素（可选）。
- 一个<domain:authInfo>元素。

<create>命令成功执行后，服务器返回响应中的EPP<resData>元素必须包含一个<domain:creData>元素，该元素包含下列子元素：

- 一个<domain:name>元素。
- 一个<domain:crDate>元素。
- 一个<domain:exDate>元素（可选）。

响应命令中还需包含<extension>元素，该元素必须包含一个<e164:create>子元素，标识e164名字空间和e164策略位置。<e164:create>元素包含一个或多个<e164:naptr>元素包含下列子元素：

- 一个<e164:order>元素，包含一个NAPTR order值。
- 一个<e164:pref>元素，包含一个NAPTR preference值。
- 一个<e164:flags>元素，包含一个NAPTR flags值（可选）。
- 一个<e164:svc>元素，包含一个NAPTR service值。
- 一个<e164:regex>元素，包含一个NAPTR regex值（可选）。
- 一个<e164:replacement>元素，包含一个NAPTR replacement值。

<create>命令应当限定给已经授权的客户使用，可被限定为每客户方式。

C. 5. 2. 2. 2 <delete>命令

除标准EPP命令元素外，<delete>请求命令必须包含一个<domain:delete>元素，标识域名字空间和域模式的位置。该元素包含以下子元素：

- 一个<domain:name>元素。

如果域对象有关联的下级主机对象，那么它不能被删除。如果出现此情况，服务器需返回代码为2305的错误响应。

当服务器成功执行<delete>命令后，返回消息中带有<resData>元素，该元素必须包含一个子元素表示对象名字空间和对象模式的位置。<resData>元素中的子元素是与具体对象相关的。

<delete>命令应限给已授权的客户使用，建议此操作限定给赞助商客户端使用。

C. 5. 2. 2. 3 <renew>命令

除标准EPP命令元素外，<renew>请求命令必须包含一个<domain:renew>元素，标识域名字空间和域模式的位置。该元素包含下列子元素：

- 一个<domain:name>元素。
- 一个<domain:curExpDate>元素。
- 一个<domain:period>元素（可选）。

<renew>响应命令中的<resData>元素必须包含<domain:renData>，该元素包含下列子元素：

- 一个<domain:name>元素。
- 一个<domain:exDate>元素（可选）。

<renew>命令应限定给已授权的客户使用；建议此操作限定给赞助客户使用。根据对象相关策略，对象延期可能不可用或受限制。

C.5.2.2.4 <transfer>命令

<transfer>请求命令中的”op”属性：

- “request”，希望担当某已知对象的赞助者。
- “cancel”，取消转让请求。

<transfer>响应命令中的”op”属性：

- “approve”，同意接受请求。
- “reject”，拒绝请求。

除标准EPP命令元素外，<transfer>请求命令必须包含一个<domain:transfer>元素，标识域名字空间和域模式的位置。该元素包含以下子元素：

- 一个<domain:name>元素。
- 一个<domain:period>元素（可选）。
- 一个<domain:authInfo>元素。

<transfer>响应中<resData>元素应包含<domain:trnData>元素，该元素与<transfer>查询响应中包含的子元素相同。转让操作必须隐含地转让对象的所有下级主机。

<transfer>命令应限定给已授权的客户端使用；建议限制<transfer>请求给当前赞助商客户端以外的客户端使用，<transfer>通过请求给当前赞助商客户端使用，<transfer>取消请求给发起请求的客户端使用。对象转让可根据对象相关策略不可用或受限。

C.5.2.2.5 <update>命令

除标准EPP命令元素外，<update>请求命令必须包含一个<domain:update>元素，标识域名字空间和域模式的位置。该元素包含以下子元素：

- 一个<domain:name>元素。
- 一个<domain:add>元素（可选）。
- 一个<domain:rem>元素（可选）。
- 一个<domain:chg>元素（可选）。

至少要有<domain:add>、<domain:rem>或<domain:chg>元素中的一个。

其中<domain:add>和<domain:rem>元素包含下列子元素：

- 一个<domain:ns>元素（可选）。
- 零个或多个<domain:contact>元素。
- 零个或多个<domain:status>元素。

<domain:chg>元素包含下列子元素：

- 一个<domain:registrant>元素。
- 一个<domain:authInfo>元素。

<extension>元素必须包含一个<e164:update>子元素，用于标识e164名字空间和e164策略的位置。<e164:update>元素包含一个或多个<e164:add>或<e164:rem>元素。每个<e164:add>和<e164:rem>元素包含一个<e164:naptr>元素，该元素包含下列子元素：

- 一个<e164:order>元素，包含一个NAPTR order值。
- 一个<e164:pref>元素，包含一个NAPTR preference值。
- 一个<e164:flags>元素，包含一个NAPTR flags值（可选）。
- 一个<e164:svc>元素，包含一个NAPTR service值。
- 一个<e164:regex>元素，包含一个NAPTR regex值（可选）。
- 一个<e164:replacement>元素，包含一个NAPTR replacement值（可选）。

<update>操作应限定给已授权的客户端使用；建议将次操作限定给赞助商客户端使用。

C.5.2.2.6 请求操作的离线复查

服务器可能会对请求执行离线复查操作，这种情况下，服务器必须明确指示消息已被接收和处理，但请求未决。相应对象的状态应当清楚地反映未决状态。当离线处理完成后，服务器必须通知客户。

返回响应之后域对象状态必须包含“pendingCreate”。服务器操作员离线复查请求完成后，需在队列中放置一条服务，供客户端的<poll>命令查看输出结果。

服务消息必须在<response>、<msgQ>、<msg>元素中包含描述该通知的文字。此外<resData>元素必须包含一个<domain:panData>元素用于标识域名字空间和域模式的位置。

此外<resData>元素必须包含<domain:panData>元素，该元素包含以下子元素：

- 一个<domain:name>元素。
- 一个<paTRID>元素。
- 一个<domain:paData>元素。

C.6 EPP结果代码

EPP 使用 4 位 10 进制数描述每个 EPP 命令的成功或失败。应答的每位数字具有特定的含义。第一位数字标识命令成功或失败。第二位数字标识响应类别，例如命令语法或安全性。第三位和第四位提供每种响应更详细的信息。

每个 EPP 响应必须包含结果代码，以及可读的结果代码描述。语言可以在<msg>元素的“lang”属性字段设置。如果未指定，则缺省为英语，标识为“en”。关于有效的“lang”属性值描述参看 RFC3066。响应文本可能被翻译成另外一种语言，翻译必须维持代码的含义，不允许更改响应代码值。

响应的第一位有两种取值：

- 1yzz — 表示肯定完成应答。该命令被接收并且被正确无误地处理。
- 2yzz — 表示否定完成应答。该命令未被接收且请求操作未被执行。

响应的第二位有六种取值：

- x0zz — 协议语法。
- x1zz — 特定实现规则。
- x2zz — 安全性。
- x3zz — 数据管理。
- x4zz — 服务器系统。
- x5zz — 连接管理。

表 C.1 返回代码表

响应代码	响应文本	响应描述
1000	"Command completed successfully "	命令成功完成且不符合其它1xxx系列响应代码的命令。
1001	"Command completed successfully; action pending"	在命令执行之前需要离线操作。
1300	"Command completed successfully; no messages"	当发起<poll>请求，服务器的消息队列为空。
1301	"Command completed successfully; ack to dequeue"	使用<poll>请求命令从服务器消息队列中取得消息。
1500	"Command completed successfully; ending session"	成功响应<logout>命令。
2000	"Unknown command"	当服务器收到EPP未定义的命令元素。
2001	"Command syntax error"	服务器收到格式不正确的命令元素。
2002	"Command use error"	服务器收到格式正确的命令元素，但由于顺序或内容错误而无法执行此命令。

表 C.1 (续)

响应代码	响应文本	响应描述
2003	"Required parameter missing"	服务器收到命令中未提供必要的参数。
2004	"Parameter value range error"	服务器收到命令参数的范围超出协议规定值的范围。应在返回的EPP响应的<value>元素中包含此错误的数值。
2005	"Parameter value syntax error"	服务器收到的命令包含的参数值格式不正确。应在返回的EPP响应的<value>元素中包含此错误的数值。
2100	"Unimplemented protocol version"	服务器收到的命令元素指定了本服务尚未实现的协议版本。
2101	"Unimplemented command"	服务器收到的有效的命令元素，但本服务器未实现该命令。例如，<transfer>命令对于某些对象类型可以不实现。
2102	"Unimplemented option"	服务器收到一条有效的EPP命令元素，该元素包含的本服务器未实现的协议选项。
2103	"Unimplemented extension"	服务器收到一条有效的EPP命令元素，包含本服务器未实现的协议扩展。
2104	"Billing failure"	服务器试图执行计费操作且由于客户端计费失败致使命令未完成。
2105	"Object is not eligible for renewal"	客户试图对一个对象使用<renew>操作，而服务器策略不允许该对象延期。
2106	"Object is not eligible for transfer"	客户试图对一个服务器策略不允许转让的对象使用<transfer>操作。
2200	"Authentication error"	服务器发现验证用户正式有效性出错。
2201	"Authorization error"	服务器发现执行一条命令时出现客户授权错误，该错误代码通常用于指示客户不具备执行该请求命令的权利。
2202	"Invalid authorization information"	服务器收到执行一条命令所需的命令授权信息是无效的。通常用于指示客户端具有执行该请求命令的权利，但客户端提供的授权信息与服务器存储的授权信息不匹配。
2300	"Object pending transfer"	服务器收到一条转让对象命令，但该对象先前的transfer请求已经挂起。
2301	"Object not pending transfer"	服务器收到一条命令用于确认、拒绝或取消一个对象的转让操作，但该对象并未执行给转让操作。
2302	"Object exists"	服务器收到一条创建对象的命令，但对象已经在数据库中。
2303	"Object does not exist"	服务器收到一条命令用于查询或变换一个数据库中不存在的对象。

表 C.1 (续)

响应代码	响应文本	响应描述
2304	"Object status prohibits operation"	服务器收到一条改变对象命令，但由于服务器策略或商业运作原因未完成。例如，服务器可以根据本地策略下条款或情况禁止<transfer>命令，或者服务器可能接收一条<delete>某个对象命令，但该对象的状态为禁止删除。
2305	"Object association prohibits operation"	服务器收到一条命令用于变换对象，但由于该与其关联的其它对象的依赖性导致无法完成操作。例如，当对象与其它对象处于活动关联状态时，服务器可以禁止<delete>操作。
2306	"Parameter value policy error"	服务器收到的命令所包含的参数在语法上有效，但对于本地策略来说在语义上是无效的。例如，服务器可能支持一个有效协议参数值的子集合。错误值应当通过<EPP>响应中的<value>元素返回。
2307	"Unimplemented object service"	服务器收到的某个在本机未实现时的对象服务操作。
2308	"Data management policy violation"	服务器收到一条命令，其执行结果与服务器数据管理策略冲突。例如，删除关联某个对象的所有属性值或对象可能与服务器的数据管理策略冲突。
2400	"Command failed"	由于内部服务器错误而并非协议原因导致无法执行一条命令。失败可以是暂时的。服务器必须保持当前所有会话是活动的。
2500	"Command failed; server closing connection"	服务器收到一条命令由于服务器内部错误而非协议原因未能完成。失败不是暂时的，它还将导致其它命令失败。服务器必须结束当前活动的会话并关闭已有连接。
2501	"Authentication error; server closing connection"	服务器在验证用户证书出错以及超出服务器定义的最大允许失败数目。服务器必须关闭已有的连接。
2502	"Session limit exceeded; server closing connection"	服务器收到<login>命令，但由于用户数已经超出服务器所规定的可建立最大会话数，导致命令无法完成。这可能会结束已有的未使用的会话或用来关闭不活动的连接来建立一个会话。

附 录 D
(资料性附录)
典型消息流程举例

D.1 PSTN用户呼叫SIP终端

利用ENUM建立一个由PSTN用户发起的到基于IP网络的SIP终端的呼叫，其典型的流程如图D.1所示：

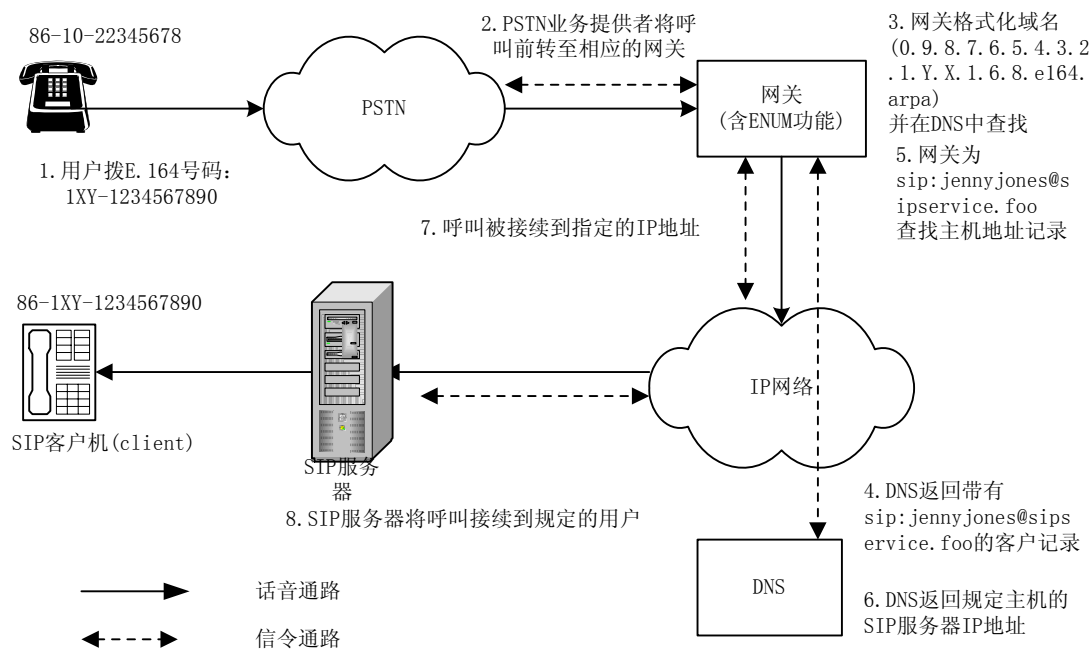


图 D.1 PSTN 用户呼叫 SIP 终端用户

步骤1：发端用户拨E. 164号码1XY1234567890；

步骤2：PSTN的业务提供者根据用户所拨号码中的1XY将呼叫转至相应的支持ENUM功能的网关, ENUM网关的物理位置需要综合考虑多方面的因素；

步骤3：该网关将用户所拨的号码按照规定的规则转换成域名，如果用户拨的号码不是全号，则网关应能够将丢掉的数字补齐，这样才能够形成一个完整、有效的域名。在本例中用户拨的号码为：1XY1234567890，完整的号码应是：861XY1234567890。然后网关在DNS中查找相应的域名；

步骤4：DNS向ENUM网关返回与该域名相关的所有业务记录；

步骤5：网关在DNS中查找指定主机的地址记录；

步骤6：DNS返回指定主机的SIP服务器的IP地址；

步骤7：通过基于IP的网络将该呼叫接续到指定的IP地址；

步骤8：SIP服务器将呼叫接续到规定用户的用户代理客户机上。

可能的消息流程如图D. 2所示：

- 步骤1：发端用户拨E. 164号码1XY0123456789，SIP客户机使用相应的“tel：”URI向SIP服务器发送SIP INVITE；
- 步骤2：SIP服务器将该电话号码转化相应的域名，并向DNS发起查询；
- 步骤3：DNS返回与该域名相关的所有NAPTR记录；
- 步骤4：如果发端和终端属于不同的IP电话管理域，SIP服务器可向位置服务器查询该电话号码对应的网关的IP地址；
- 步骤5：位置服务器返回与目的地号码对应的网关的IP地址；
- 步骤6：SIP服务器使用新的“tel：”URI向网关发送SIP INVITE；
- 步骤7：IP网络将呼叫接续到指定IP地址的网关；
- 步骤8：网关通过PSTN完成到目的地的电话呼叫。网关将对来自PSTN的任何信令（如回铃音、忙等）都做出响应，并且将相应的信息返回给呼叫的发起者。
- 可能的消息流程如图D. 4所示：

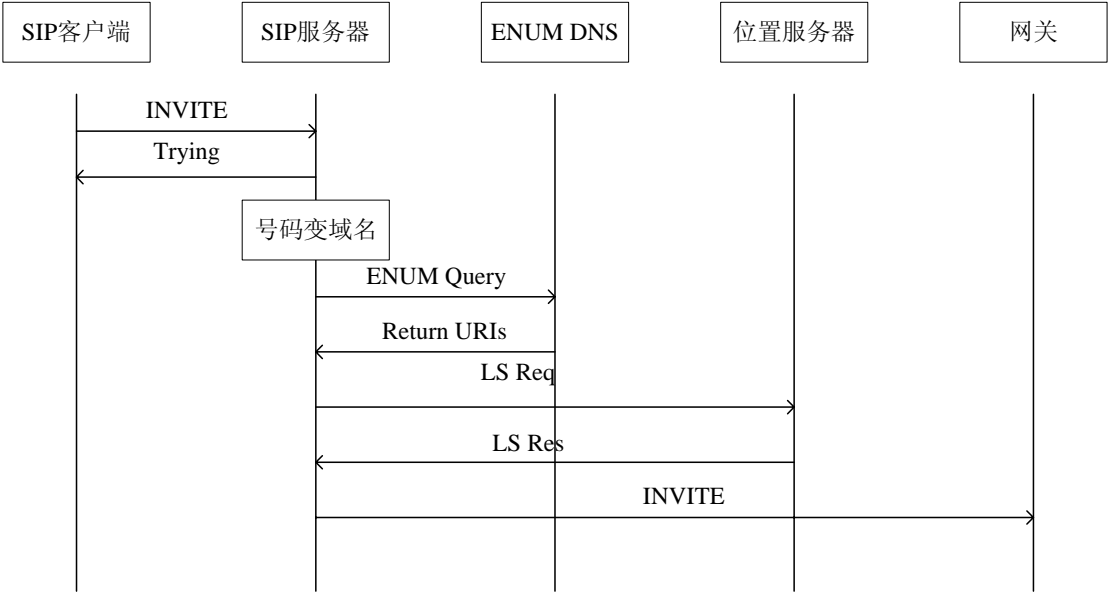


图 D. 4 SIP 终端呼叫 PSTN 用户时可能的消息流程

D. 3 多媒体消息业务

- 在多媒体消息业务中，基于DNS-ENUM进行接收方的MSISDN地址的解析，其流程如下：
- 1) 发起方MMS Relay/Server应确认接收方地址（MSISDN）与E. 164地址的格式一致并且包含符号“+”。对于国内或本地号码，MMS Relay/Server 应将国内或本地号码转换为完整的E. 164号码，例如：+86-1XY-1234567890。
 - 2) 发起方MMS Relay/Server去掉除“+”号之外的所有非数字字符。例如：+861XY1234567890。
 - 3) 发起方MMS Relay/Server去掉除数字之外的所有字符。例如：861XY1234567890。
 - 4) 发起方MMS Relay/Server在数字之间插入“.”，例如：8.6.1.X.Y.1.2.3.4.5.6.7.8.9.0。
 - 5) 发起方MMS Relay/Server 翻转数字的顺序，例如：0.9.8.7.6.5.4.3.2.1.Y.X.1.6.8。
 - 6) 在第5步结果的基础上追加一个后缀，例如e164. arpa，使其转化为一个FQDN。
例如：0.9.8.7.6.5.4.3.2.1.Y.X.1.6.8. e164. arpa. （公共顶级域）。
 - 7) 所获得的FQDN与符合上面步骤2所规定的格式的字串（E. 164号码）一起将被发起方MMS Relay/Server用作NAPTR算法的输入。
 - 8) 输出将导致下列情况之一：

- 没有与该号码对应的URI。始发方MMS Relay/Server 将调用相应的地址解析例外处理程序（例如：向始发方MMS User Agent发送一个消息报告该差错情况，执行必要的转换，并且将该消息选路至接收方等）；
- 没有与该号码对应的MMS URI（MMS URI的格式为“mms: mailbox”，并且它们是在MMS 资源记录部分定义的）。始发方MMS Relay/Server 将调用相应的地址解析例外处理程序（例如：向始发方MMS User Agent发送一个消息报告该差错情况，执行必要的转换，并且根据“业务字段”将该消息选路至接收方等）；
- DNS ENUM 业务不可用。始发方MMS Relay/Server 将调用相应的地址解析例外处理程序（例如：向始发方MMS User Agent发送一个消息报告该差错情况，将该消息存储在队列中，晚些时候重试等）；
- 存在与该号码对应的MMS URI。与从接收方的MSISDN地址（例如+306971234567）衍生而来的与FQDN相关联的NAPTR资源记录举例如下：

```
IN NAPTR 100 10 "u" "E2U+sip" "!.*$!sip: Mary.Smith@sip.cosmote.gr!".
IN      NAPTR      100      11      "u"      "E2U+mms"      "!.*$!mms      :
+306971234567/TYPE=PLMN@mms.cosmote.gr!".
IN NAPTR 101 10 "u" "E2U+mailto" "!.*$!mailto: Mary.Smith@mycosmos.gr!".
IN NAPTR 102 10 "u" "E2U+mailto" "!.*$!mailto: MaryS@otenet.gr!".
```

根据以上的记录，+861XY1234567890被转换为以下的URI：

```
sip: Mary.Smith@sip.cosmote.gr
mms: +306971234567/TYPE=PLMN@mms.cosmote.gr
mailto: Mary.Smith@mycosmos.gr
mailto: MaryS@otenet.gr
```

- 9) 如果ENUM-DNS返回一个以上的URI，则发起方MMS Relay/Server 将根据“Order”和“Preference”字段对MMS URI进行排序。
- 10) 发起方MMS Relay/Server 将对具有最高优先级的MMS URI的“mailbox”的域部分进行解析，使用标准的DNS将其解析为IP地址。例如具有最高优先级的MMS URI为：
mms: +306971234567/TYPE=PLMN@mms.cosmote.gr
该“mailbox”的域部分为：mms.cosmote.gr，它被解析为：10.10.0.1
- 11) 作为解析结果的IP地址和接收方的mailbox地址一起被发起方MMS Relay/Server用于将多媒体消息选路至接收方MMS Relay/Server。

NAPTR 资源记录 (RR) 中的关键字段是域 TTL、Class、Type、Order、Preference、Flags、Service、Regexp 和 Replacement。这些字段在 IETF 的相关文件中都进行了规定，在 3G 的相关文件中对以下的字段作了进一步的规定：

Service = "E2U+mms"

Regexp = "!.*\$!mms: mailbox!" 其中“mailbox”以及相关的格式规则在 IETF 的相关文件中 (RFC 2822) 规定。

MMS URI的形式为“mms: mailbox”。