



中华人民共和国通信行业标准

YD/T 2908-2015

基于域名系统(DNS)的 IP 安全协议认证 密钥存储技术要求

Technical requirements for DNS-based IP
Sec keying material storage

2015-10-14 发布

2016-01-01 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 术语、定义和缩略语..... 1

 3.1 术语和定义..... 1

 3.2 缩略语..... 1

4 概述..... 2

5 存储格式..... 2

 5.1 RDATA 结构..... 2

 5.2 优先级..... 2

 5.3 网关类型..... 2

 5.4 算法..... 3

 5.5 网关..... 3

 5.6 公钥..... 3

6 呈现格式..... 4

7 安全考量..... 4

 7.1 资源记录安全性分析..... 4

 7.2 针对不安全的 IPSECKEY 资源记录的主动攻击..... 4

附录 A（资料性附录） IPSECKEY 资源记录举例..... 6

参考文献..... 7

前 言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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：互联网域名系统北京市工程研究中心有限公司、北龙中网（北京）科技有限责任公司、中国科学院计算机网络信息中心（中国互联网络信息中心）。

本标准主要起草人：马 迪、钱炜烁、沈 烁、邢志杰、卢文哲、毛 伟。

本标准主要参考 IETF RFC 4025，同时存在以下差异：

——将 IETF RFC 4025 的举例章节放到了资料性附录。

——为了方便读者理解，本标准 5.3 中对“线性编码域名”一词加以简要说明。

基于域名系统(DNS)的 IP 安全协议认证密钥存储技术要求

0 范围

本标准规定了一种基于DNS的IPSec认证密钥及加密点信息存储方法，该方法可用于从DNS权威服务器获取IPSec目标系统的密钥信息和加密点信息。本标准规定了该资源记录的数据格式及其使用方法。

本标准适用于部署有安全的DNS服务（通过DNSSEC或类似技术实现）的系统。

0 规范性引用文件

下列文件对于本文件的应用是必不可少的。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。

IETF RFC 596 关于Telnet许可的重考虑（Second Thoughts on Telnet Go-Ahead）

IETF RFC 1035 域名——实现与规范（DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION）

IETF RFC 2407 ISAKMP的IPSec解释域（The Internet IP Security Domain of Interpretation for ISAKMP）

IETF RFC 2536 域名系统的DSA密钥和签名（DSA KEYs and SIGs in the Domain Name System (DNS)）

IETF RFC 3110 域名系统的RSA/SHA-1签名与RSA密钥（RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)）

IETF RFC 3548 Base16、Base32与Base64编码（The Base16, Base32, and Base64 Data Encodings）

0 术语、定义和缩略语

0.0 术语和定义

下列术语和定义适用于本文件。

0.0.0

客户端 Client

用来建立连接用来发送请求的一个程序。

0.0.0

资源记录 Resource Record

每个域所包含的与之相关的资源

0.0 缩略语

下列缩略语适用于本文件。

DNS	Domain Name System	互联网域名系统
IP	Internet Protocol	互联网协议
IPSec	Internet Protocol Security	IP 安全协议
PTR	Pointer Record	反向地址解析资源记录
RSA	RSA Algorithm	RSA 加密算法
DSA	Digital Signature Algorithm	数字签名算法

IKSAKMP	Internet Security Association and Key Management Protocol	互联网安全关联钥匙管理协议
IKE	Internet Key Exchange	因特网密钥交换
NAT	Network Address Translation	网络地址转换
NAPT	Network Address and Port Translation	网络地址与端口转换

0 概述

在目前的网络环境下，IPSec是保障主机之间安全通信的重要手段之一，也是部署最为广泛的IP层安全技术。

假设有这样一台主机（可能是出于政策要求或者技术规范），必须首先与目标设备建立IPSec隧道连接，然后才能进行正常的通信。在多数情况下，这台主机是有办法确切地获知目标设备的DNS域名的。要么是显式地得知DNS域名；要么是针对一个特定的IP地址执行DNS PTR查询；或者通过其他方式，例如：通过提取目标设备的“user@FQDN”名称中的DNS有关的部分。

在上述这些情形中，该主机都有必要获取一个公钥来验证该目标主机；有时候，它还需要获得一些指示信息，以便决定自己是应该直接与目标主机联系，还是通过另一个作为网关的节点来间接地联系目标主机。

0 存储格式

0.0 RDATA 结构

IPSECKEY资源记录中的RDATA包括：优先级、网关类型、公钥值、算法类型、以及网关地址（可选）。如图1所示。

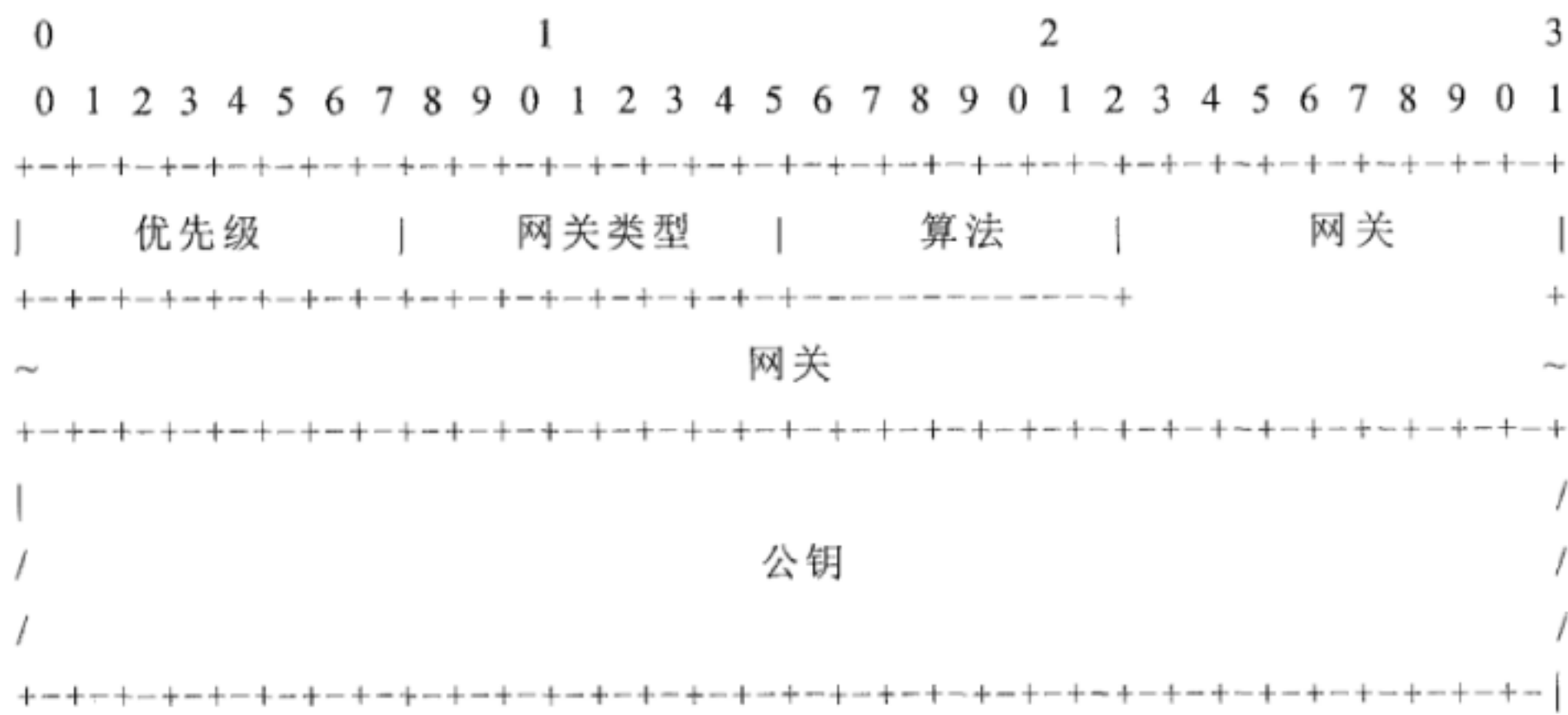


图0 IPSECKEY 资源记录的 RDATA 结构

0.0 优先级

这是一个8比特字段，用于标识该记录的优先级；其意义参见IETF RFC 1035第3.3.9小节。
如有多条 IPSECKEY 资源记录可用，则其中存储的网关地址将按照记录的优先级数值递增顺序依次被尝试；如果两个网关地址的优先级相同，那么实际顺序将取决于具体实现。

0.0 网关类型

网关类型字段指示网关字段所存储内容的格式。
一共定义了以下几个可能的值：

- 0: 无网关;
- 1: 一个 4 字节的 IPv4 地址;
- 2: 一个 16 字节的 IPv6 地址;
- 3: 一个线性编码域名 (开头用一个字节来存储域名中包含的字符个数, 即长度; 后面跟着指定长度的字符串表示具体的域名)。

由于线性编码域名是自描述的, 所以其长度也是隐含可知的。该域名不得压缩。

5.4 算法

算法字段指示公钥所使用的加密算法及其格式。

定义了以下几个可能的值:

- 0: 无密钥;
- 1: 采用 DSA 密钥, 见 IETF RFC 2536 中规定的格式;
- 2: 采用 RSA 密钥, 见 IETF RFC 3110 中规定的格式。

5.5 网关

网关字段存储一个网关地址, 通过与该网关地址建立IPSec隧道连接, 可以与资源记录中指定的实体通信。

一共定义了3种格式:

- 网关字段存储一个 32 位的 IPv4 地址, 其数据部分是一个按照 IETF RFC 1035 中第 3.4.1 小节规定的 IPv4 地址。这是一个 32 位的数字, 按照网络字节序存储。
- 网关字段存储一个 128 位的 IPv6 地址, 其数据部分是一个按照 IETF RFC 596 中第 2.2 节规定的 IPv4 地址。这是一个 128 位的数字, 按照网络字节序存储。
- 网关字段存储一个线性编码的域名, 按照 IETF RFC 1035 中第 3.3 节规定的格式存储。域名不得压缩。

5.6 公钥

本标准中定义的两公钥类型 (RSA和DSA), 都完全遵照其相应的KEY资源记录中的格式。具体说来, 公钥字段包含的是KEY资源记录中的算法特定部分, 即KEY资源记录中开头4个字节后面的全部数据。这也是KEY资源记录中, 应被DNSSEC算法定义文档所详细规定的部分。此类文档同时也会规定一种消息摘要算法, 用于生成SIG资源记录; 不过, 这些消息摘要算法相关的规定与IPSECKEY资源记录无关。

未来如果有新的加密算法产生, 且打算被DNSSEC (在KEY资源记录中) 和IPSECKEY资源记录同时采用, 则它们将很可能沿用这两种记录中现成的公钥编码方式。除非特别说明, IPSECKEY资源记录中的公钥字段格式不变。该算法应仍然是针对IPSECKEY资源记录应用设计的, 且应为其赋予相应的IPSECKEY算法类型编码; 这个编号可以跟DNSSEC中的算法编号不同。

DSA密钥格式依照RFC2536规定, RSA密钥格式依照IETF RFC 3110规定。有以下改动:

IETF RFC 2065中关于RSA/MD5的早期规定是, 指数和模数不得超过2552比特。IETF RFC 3110中针对RSA/SHA1, 将这一限制放宽到4096比特。而在IPSECKEY资源记录中, 对RSA的公钥长度则几乎全无限制; 只有2字节长度编码所导致的65535字节长度限制。该长度限制的放宽仅针对IPSECKEY资源记录有效; 对KEY资源记录无效。

6 呈现格式

IPSECKEY资源记录可能存储在一个DNS区文件中。优先级、网关类型、算法和网关字段是强制要求的；用Base64编码加密过的公钥块则是可选的。如果并未指定公钥，则资源记录的公钥字段应是0字节长。算法字段是一个无符号整数。没有定义相应的助词符。

如果没有指定网关，则“网关类型”字段应置零，且“网关”字段应置为“.”。

“公钥”字段是以经Base64编码的公钥格式存储的。Base64格式中允许空白字符。关于Base64的详细定义，见IETF RFC 3548第5.2节。

IPSECKEY资源记录的通用呈现格式如下：

IN IPSECKEY (优先级 网关类型 算法
 网关 基于Base64编码的公钥)

示例参见附录A。

0 安全考量

0.0 资源记录安全性分析

本标准所涉及的一切公钥信息交换，皆通过密钥管理协议来实现。例如，ISAKMP/IKE协议（见IETF RFC 2407）。

IPSECKEY资源记录中所存储的信息应当被完整地、无修改地传递给客户端。传递的方式取决于该信息的使用者。该资源记录的服务器和终端用户之间应存在某种信任关系。该信任关系可能是端到端的DNSSEC验证、一条指向另一个安全信息源的TSIG或者SIG (0)隧道、或者是一条主机上的本地安全信道；也可能是上述各种方法的灵活组合。

IPSECKEY资源记录所提供的密钥信息可抗被动攻击。公钥信息可以随意分发给任意第三方，而不会给IPSec会话的安全性造成任何影响。IPSec和IKE提供了针对主动攻击和被动攻击的保护。

基于本资源记录的任何衍生规范应在其文档中仔细地说明其采用的信任模型；如果要采用DNSSEC信任模型，应证明采用该信任模型的合理性。

假设存在针对DNS的主动攻击，导致客户端查到错误的地址（地址伪造），进而查询错误的QNAME记录，将最终导致中间人攻击。然而，此种问题的存在与是否采用IPSECKEY资源记录并无关系。

0.0 针对不安全的 IPSECKEY 资源记录的主动攻击

0.0.0 总论

7.2条讨论针对DNS的主动攻击。此类攻击需要抓取并篡改DNS请求和响应报文。DNSSEC可用于抵抗此类攻击。本条要讨论的是DNSSEC不可用的环境下的问题，而这并不是我们推荐的部署环境。

0.0.0 针对 IPSECKEY 公钥信息的主动攻击

第一种主动攻击方式就是，攻击者把公钥信息换成自己控制的密钥或者一段垃圾信息。

至于网关字段，要么是未改动、或者是null。这样，IKE协商过程将与原始终端系统直接进行。此类攻击若要成功，攻击者应针对IKE协商过程实施中间人攻击。而这种攻击，要求攻击者有能力在IKE和通信内容数据包的转发路径上截获并篡改数据包。

如果攻击者无法实施这一针对IKE协商过程的中间人攻击，则IKE协商过程失败，导致“拒绝服务攻击”。

如果攻击者不仅能发起针对DNS的主动攻击，还处于一个能够对IKE和IPSec协商过程实施中间人攻击的网络节点位置，那么攻击者将有能力破坏IPSec信道。需要注意的是，攻击者应有能力同时对IKE协商的两端实施DNS主动攻击，才能最终成功。

0.0.0 针对 IPSECKEY 网关信息的主动攻击

第二种攻击，是攻击者篡改网关地址，使其指向自己控制的机器。然后，攻击者要么换掉公钥、要么删除公钥。如果公钥被删除了的话，攻击者可以在另外一条记录中提供自己的公钥。

这种攻击方式会造成一个简单的中间人攻击，因为攻击者可以随后与真实的目标节点建立一条旁路信道。请注意，与上述情形一样，这也要求攻击者同时还能对响应者发起主动攻击。

请注意，中间人仅仅把明文数据包转发给真实的目标设备是不够的。因为，当目标设备把“自己期望明文通信”返回给发送端设备的时候，发送端设备可能已经设置好了“期待加密通信”的政策。因此，攻击者不得不侵入双向的通信流量。在某些情况下，攻击者可以通过地址/端口映射（NAT/NAPT）来实现全面的入侵。

这种攻击方式比第一种要容易一些，因为攻击者不必处于端到端的转发路径上。攻击者只要能篡改DNS应答数据包就可以了。这是比较容易实现的，可以通过各种数据包篡改技术、或者攻击DNS缓存就可以实现。

如果IPSECKEY资源记录的端到端完整性受到怀疑，那么客户端应限制IPSECKEY资源记录的使用；只有当资源记录持有者的域名跟网关字段相匹配时才可以使用。因为，当资源记录持有者域名中的网关部分为空时，IPSECKEY资源记录中的网关字段应为空，才被视为合法的匹配。

这样一来，在未验证的情况下（没有DNSSEC或者通往发送者的信任链）获取的任何非空的“网关”字段应被忽略。

这条规则有效地消除了针对网关字段的攻击。而这一攻击被认为是容易得多的，因为攻击者并不需要处于转发路径上。

当IPSECKEY资源记录中“网关类型”字段的值为3时，网关字段保存的将是一个域名。接下来，把这个域名翻译为IP地址或者IPSECKEY资源记录的后续查询交互也将成为中间人攻击的目标。如果第二个查询的端到端完整性受到怀疑，则上述的规则仍然适用。即，当查到的网关地址与最开始的IPSECKEY资源记录查询中的QNAME不一致时，该IPSECKEY资源记录将被丢弃。

附录 A

(资料性附录)

IPSECKEY 资源记录举例

示例1: 某节点地址为 192.0.2.38, 接受以自己为加密点的 IPSec 隧道, 其 IPSECKEY 资源记录如下:

```
38.2.0.192.in-addr.arpa.          7200
IN IPSECKEY (10 1 2
    192.0.2.38 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ==)
```

示例2: 某节点地址为 192.0.2.38, 仅发布其公钥。其 IPSECKEY 资源记录如下:

```
38.2.0.192.in-addr.arpa.          7200
IN IPSECKEY (10 0 2
    . AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ==)
```

示例3: 某节点地址为 192.0.2.38, 已经将自己的权威授权给 192.0.2.3 节点, 以该节点来代表 IPSec 隧道。其 IPSECKEY 资源记录如下:

```
38.2.0.192.in-addr.arpa.          7200
IN IPSECKEY (10 1 2
    192.0.2.3 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ==)
```

示例4: 某节点地址为 192.0.1.38, 已经将自己的权威授权给域名为 "mygateway.example.com" 的节点。其 IPSECKEY 资源记录如下:

```
38.1.0.192.in-addr.arpa.          7200
IN IPSECKEY (10 3 2
    mygateway.example.com. AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ==)
```

示例5: 某节点地址为 2001:0DB8:0200:1:210:f3ff:fe03:4d0, 已经将自己的权威授权给 2001:0DB8:c000:0200:2::1 节点。

其 IPSECKEY 资源记录如下:

```
$ORIGIN 1.0.0.0.0.2.8.B.D.0.1.0.0.2.ip6.arpa.
0.d.4.0.3.0.e.f.f.3.f.0.1.2.0      7200
IN IPSECKEY (10 2 2
    2001:0DB8:0:8002::2000:1 AQNRU3mG7TVTO2BkR47usntb102uFJtugbo6BSGvgqt4AQ==)
```

参 考 文 献

[0] IETF RFC 2065 Domain Name System Security Extensions

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
高速分组数据（HRPD）（第四阶段）空中接口测试方法
信令一致性

YD/T 3043-2016

*

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

北京康利胶印厂印刷

版权所有 不得翻印

*

开本：880×1230 1/16

2016 年 9 月第 1 版

印张：8

2016 年 9 月北京第 1 次印刷

字数：219 千字

15115 • 1027

定价：80 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492