

中华人民共和国通信行业标准

YD/T 2586-2013

域名服务系统安全扩展 (DNSSEC) 协议和实现要求

Security extensions of DNS and implementation requirement

2013-07-22 发布

2013-10-01 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
4 域名系统安全扩展 (DNSSEC)	3
5 DNSSEC 新增的资源记录类型	4
6 DNSSEC 对 DNS 协议的修改	8
7 DNSSEC 的部署实施要求	9
附录 A (资料性附录) DNSSEC 原理举例说明	10
附录 B (资料性附录) DNSSEC 国际部署情况	11
附录 C (资料性附录) DNSSEC 实例	12
附录 D (资料性附录) 密钥标签字段计算方法	21
参考文献	22

前 言

本标准按照 GB/T1.1-2009 给出的规则起草。

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：工业和信息化部电信研究院、中国互联网络信息中心、国家计算机网络应急技术处理协调中心。

本标准主要起草人：陈 浩、田慧蓉、姚健康、沈 烁。

域名服务系统安全扩展（DNSSEC）协议和实现要求

1 范围

本标准针对域名服务系统安全扩展的功能、协议和工作原理进行了详细的规定，并提出了 DNSSEC 部署实施的要求。

本标准适用于域名服务系统的安全扩展。

2 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。

YD/T 2140-2010 域名服务系统安全框架技术要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

区签名密钥 Zone Signing Key

对权威域数据进行DNSSEC签名或验证的密钥对。通常，相对于密钥签名密钥，区签名密钥比较短，具有较短的有效期，但是具有较高的签名效率。

3.1.2

密钥签名密钥 Key Signing Key

对区签名密钥对中的公钥进行数字签名或验证的密钥对。通常，相对于区签名密钥，密钥签名密钥比较长，具有较长的生存期，但签名效率较低。

3.1.3

DNS公钥（DNSKEY） DNS Public Key

DNSKEY资源记录存储的是权威域的公钥。权威域使用私钥对DNS资源记录集进行数字签名，并且将公钥保存在DNSKEY资源记录中，用于稍后对数字签名的验证。

3.1.4

资源记录签名（RRSIG） Resource Record Signature

RRSIG资源记录存储的是DNS资源记录集的数字签名。

3.1.5

授权签名者（DS） Delegation Signer

DS资源记录存储了DNSKEY资源记录的散列值，用于建立解析服务器验证DNS应答报文时所需的信任链，它可以验证与之对应的DNSKEY资源记录。

3.1.6

信任锚 Trust Anchor

一个预先配置的DNSKEY资源记录或者DNSKEY资源记录的散列值（DS资源记录）。一个支持DNSSEC的解析服务器可以使用这个公钥或者散列值作为信任链的起始点。此外，解析服务器应该通过DNS协议之外的安全可信的方法获得信任锚的初始值。

3.1.7**信任链 Authentication Chain**

一个由DNSKEY和DS资源记录交替组成的序列，DNSKEY用于验证包含DS的资源记录集签名，使得DS得到验证。DS包含了另一个DNSKEY的散列值，新的DNSKEY如果与DS的散列值匹配，也可以得到验证。这个新的DNSKEY反过来又可以验证另一个DS，这样延续下去直到获得需要验证的DNS数据签名的公钥为止。

3.1.8**支持DNSSEC的权威域名服务器 Security-Aware Name Server**

一个具有权威域名服务器功能的实体，并能够支持本标准定义的域名服务系统安全扩展(DNSSEC)。一个支持DNSSEC的权威域名服务器可以接受DNS查询报文，发送DNS应答报文，支持本标准定义的DNSSEC资源记录类型，支持DNS扩展机制等。

3.1.9**支持DNSSEC的递归域名服务器 Security-Aware Recursive Name Server**

具有递归功能的支持DNSSEC的权威域名服务器，既可以充当权威域名服务器，又可以充当解析服务器。

3.1.10**支持DNSSEC的解析服务器 Security-Aware Resolver**

一个具有DNS解析服务器功能的实体，并能够支持本标准定义的域名服务系统安全扩展(DNSSEC)。一个支持DNSSEC的解析服务器可以接受DNS查询报文，发送DNS应答报文，支持本标准定义的DNSSEC资源记录类型，支持DNS扩展机制等。

3.2 缩略语

下列缩略语适用于本文件。

AD	Authenticated Data	已验证数据
CD	Checking Disabled	关闭检查
DNS	Domain Name System	域名服务系统
DNSSEC	DNS Security Extension	域名服务系统安全扩展
DNSKEY	DNS Public Key	DNS公钥
DO	DNSSEC OK	域名服务系统安全扩展开启
DS	Delegation Signer	授权签名者
EDNS0	Extension Mechanisms for DNS	DNS扩展机制
IPSEC	Internet Protocol Security	因特网协议安全
KSK	Key Signing Key	密钥签名密钥
NSEC	Next Secure	下一个安全记录

NSEC3	Next Secure version 3	下一个安全记录第三版
RRSIG	Resource Record Signature	资源记录签名
SOA	Start Of Authority	初始授权机构
TSIG	Transaction Signatures	事务签名
ZSK	Zone Signing Key	区签名密钥

4 域名系统安全扩展 (DNSSEC)

域名系统安全扩展 (DNSSEC) 可以提供 DNS 数据源鉴别和完整性保护, 以及 DNS 数据的否定存在验证机制。本章的重点是 DNSSEC 的原理、提供的安全服务和它的局限性。

引入 DNSSEC 需要改变现有的 DNS 协议。DNSSEC 增加了 4 种新的资源记录类型, 它们是资源记录签名 (RRSIG)、DNS 公钥 (DNSKEY)、授权签名者 (DS) 和下一个安全记录 (NSEC)。但是根据 IETF RFC 5155《散列的 DNSSEC 否定存在验证》, NSEC 已经被证明是不安全的, 攻击者可以通过 NSEC 获得权威域中存在的所有域名记录。因此, 本标准将使用下一个安全记录第三版 (NSEC3)。此外, DNSSEC 在报文头增加了 2 个标志位——CD 标志位和 AD 标志位。为了支持增加了 DNSSEC 资源记录而变得更长的 DNS 报文, DNSSEC 需要 DNS 扩展机制 (EDNS0) 的支持。最后, DNSSEC 还需要使用报文头的 DO 标志位, 使得支持 DNSSEC 的解析服务器能够在其请求中指明它希望接收到的 DNSSEC 资源记录类型。

DNSSEC 原理举例说明、DNSSEC 国际部署情况以及 DNSSEC 实例参见附录 A、B、C。

4.1 DNSSEC 的基本原理

DNSSEC 协议是一个针对 DNS 协议的安全扩展, 它通过给 DNS 的应答消息添加基于非对称加密算法的数字签名来保证数据未经篡改且来源正确; 再通过域名体系自下而上逐级向父域提交自己公共密钥来实现整个域名体系的逐级安全认证。DNSSEC 本质上是在域名系统树型授权体系的基础上, 再建立一套基于密码学手段的签名/验证体系, 也就是信任链体系, 通过信任链上的逐级安全验证来确保 DNS 查询结果的真实可靠性 (数据完整性和数据源鉴别)。

DNSSEC 的基本原理是权威域名服务器用区签名密钥对中的私钥 (以下简称私钥) 对应答报文中的资源记录集进行签名, 并将资源记录集和数字签名放入同一个应答报文中, 发送给解析服务器。解析服务器用权威域的区签名密钥对中的公钥 (以下简称公钥) 对收到的应答报文进行验证。如果验证失败, 表明这一报文可能是假冒的, 或者在传输过程、缓存过程中被篡改。

4.2 DNSSEC 提供的安全服务

4.2.1 数据源鉴别和完整性保护

DNSSEC 通过对 DNS 资源记录集进行数字签名实现数据源鉴别。这个数字签名保存在一个新的资源记录类型中——RRSIG。通常情况下, 只有一个私钥对一个权威域的数据进行签名, 但也不排除使用多个密钥的可能。例如, 每一种数字签名算法都有一个密钥。如果一个支持 DNSSEC 的解析服务器获得了一个权威域的公钥, 那么它就可以验证这个权威域的签名。

支持 DNSSEC 的解析服务器可以有两种方式获得一个权威域的公钥, 一种方式是通过预先配置在解析服务器中的信任锚, 另一种是通过正常的 DNS 解析方式。在后一种方式中, 公钥被保存在 DNSKEY 中。为了保证通过 DNS 解析方式获得公钥的真实性, 该公钥还需要由一个经过认证的、预先配置的密钥签名, 即密钥签名密钥 (KSK)。因此, 支持 DNSSEC 的解析服务器为了验证签名, 需要形成一个信任链, 从新获得的权威域公钥到密钥签名密钥 (预先配置或者提前取得), 所以, 解析服务器至少需要配置

一个信任锚。

如果配置的信任锚是一个权威域的区签名密钥 (ZSK)，那么解析服务器就可以鉴别权威域数据的真实性和完整性。如果配置的信任锚是密钥签名密钥 (KSK)，那么解析服务器就可以验证权威域公钥的真实性和完整性。

如果可能，权威域的私钥应该离线保存，但是对于动态更新的权威域是不可能做到的。在动态更新的情况下，权威域的主服务器需要在更新之后重新签名 DNS 资源记录集，那么区签名密钥 (ZSK) 就不得不保存在线上。在这种情况下，使用密钥签名密钥 (KSK) 作为权威域的信任锚是有必要的。将密钥签名密钥 (KSK) 离线保存，并对区签名密钥 (ZSK) 签名，即使区签名密钥 (ZSK) 应保存在线上，也能保护它的真实性和完整性。离线保存的密钥签名密钥 (KSK) 可以使用更长时间，解决了频繁更换密钥带来的密钥分发问题。

4.2.2 否定存在验证

4.2.1 描述的安全机制只能对权威域中存在的资源记录集进行数字签名，为了能够提供 DNS 数据否定存在验证服务，DNSSEC 还需要一个新的资源记录类型——NSEC3。NSEC3 可以使支持 DNSSEC 的解析服务器能够验证某个域名或某个资源记录类型不存在的应答报文，其认证机制和解析服务器认证其他应答报文的机制一样。使用 NSEC3 需要权威域内的域名按照规范排序，NSEC3 链可以清晰地描述权威域内存在的域名，以及这些域名中有哪些资源记录类型。每一个 NSEC3 资源记录都会被签名，并有对应的 RRSIG 资源记录。

4.3 DNSSEC 不提供的安全服务

DNS 在最初设计的时候假设：不论是谁发送的特定查询请求，DNS 都将返回相同的应答，而且 DNS 保存的所有数据都是可见的。所以，DNSSEC 不提供机密性、访问控制列表或者其他区别查询者的服务。

同时，DNSSEC 不能抵抗对域名服务系统的拒绝服务攻击。

5 DNSSEC 新增的资源记录类型

本章将详细规定 DNSSEC 的 4 种资源记录类型：DNSKEY、RRSIG、NSEC3 和 DS，包括定义、功能以及资源记录的报文格式。其中的密钥标签字段计算方法参见附录 D。

5.1 DNSKEY 资源记录

DNSKEY 资源记录存储的是权威域的公钥。权威域使用私钥对 DNS 资源记录集进行数字签名，并且将公钥保存在 DNSKEY 资源记录中，用于稍后对数字签名的验证。

DNSKEY 资源记录的类型值是 48。DNSKEY 没有特殊的生命周期要求。

DNSKEY 资源记录的报文格式如图 1 所示，包括 16 比特的标志位 (Flags)，8 比特的协议字段 (Protocol)，8 比特的算法字段 (Algorithm) 和公钥字段 (Public Key)。

● 标志位

标志位的第 7 位是区密钥位，如果第 7 位为“1”，则 DNSKEY 资源记录保存的是一个权威域的公钥，该密钥可以用于签名数据的验证，而且签名数据的所有者应是该权威域。如果第 7 位为“0”，则 DNSKEY 资源记录中保存是其他类型的 DNS 密钥，不能用于对签名数据的验证。

标志位的第 15 位是安全入口点，如果第 15 位为“1”，DNSKEY 资源记录保存的密钥将作为一个安全入口点。

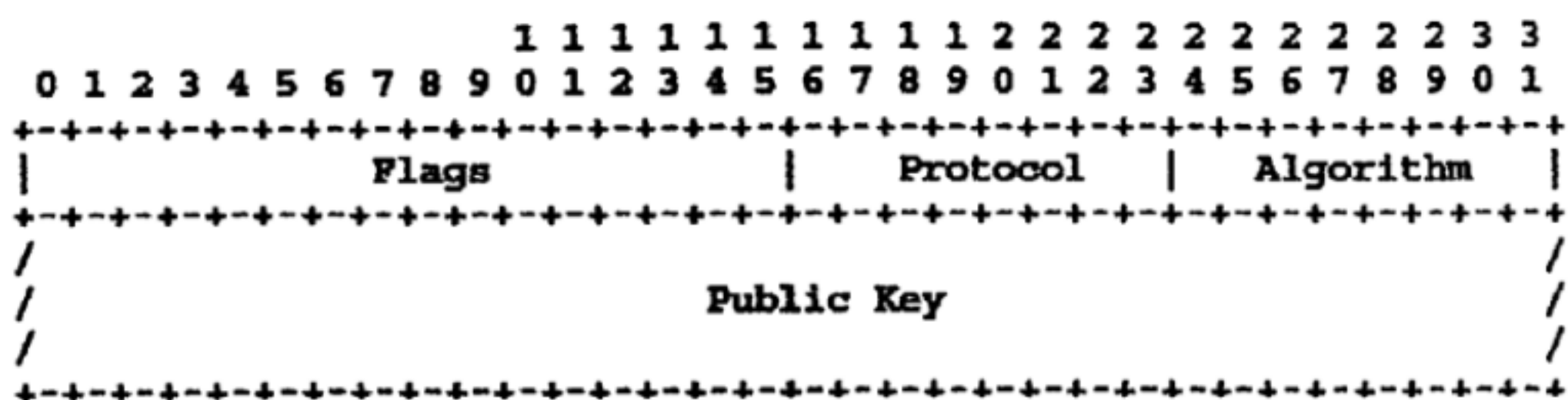


图1 DNSKEY的报文格式

标志位第 0~6bit 和第 8~14bit 保留，使用时应置为“0”。

- 协议字段

协议字段的值应是“3”，表示这是一个 DNSKEY，这是为了与以前版本 DNSSEC 兼容而保留下来的。其他的值不能用于 DNSSEC 签名的验证。

- 算法字段

算法字段表明签名所使用的算法种类，同时决定公钥字段的格式。

- 公钥字段

该字段保存的是权威域的公钥，其格式由所选取的算法决定。

5.2 RRSIG 资源记录

RRSIG 资源记录存储的是 DNS 资源记录集的数字签名。

RRSIG 资源记录的类型值是“46”。

RRSIG 资源记录的生命周期应和其覆盖的 DNS 资源记录集保持一致。

RRSIG 资源记录的报文格式如图 2 所示，包括 16 比特的类型覆盖字段 (Type covered)、8 比特的算法字段 (Algorithm)、8 比特的域名字段 (Labels)、32 比特的原始生命周期字段 (Original TTL)、32 比特的签名过期时间字段 (Signature Expiration)、32 比特的签名开始时间字段 (Signature Inception)、16 比特的密钥标签字段 (Key Tag)、签名者字段 (Signer's Name) 和签名字段 (Signature)。

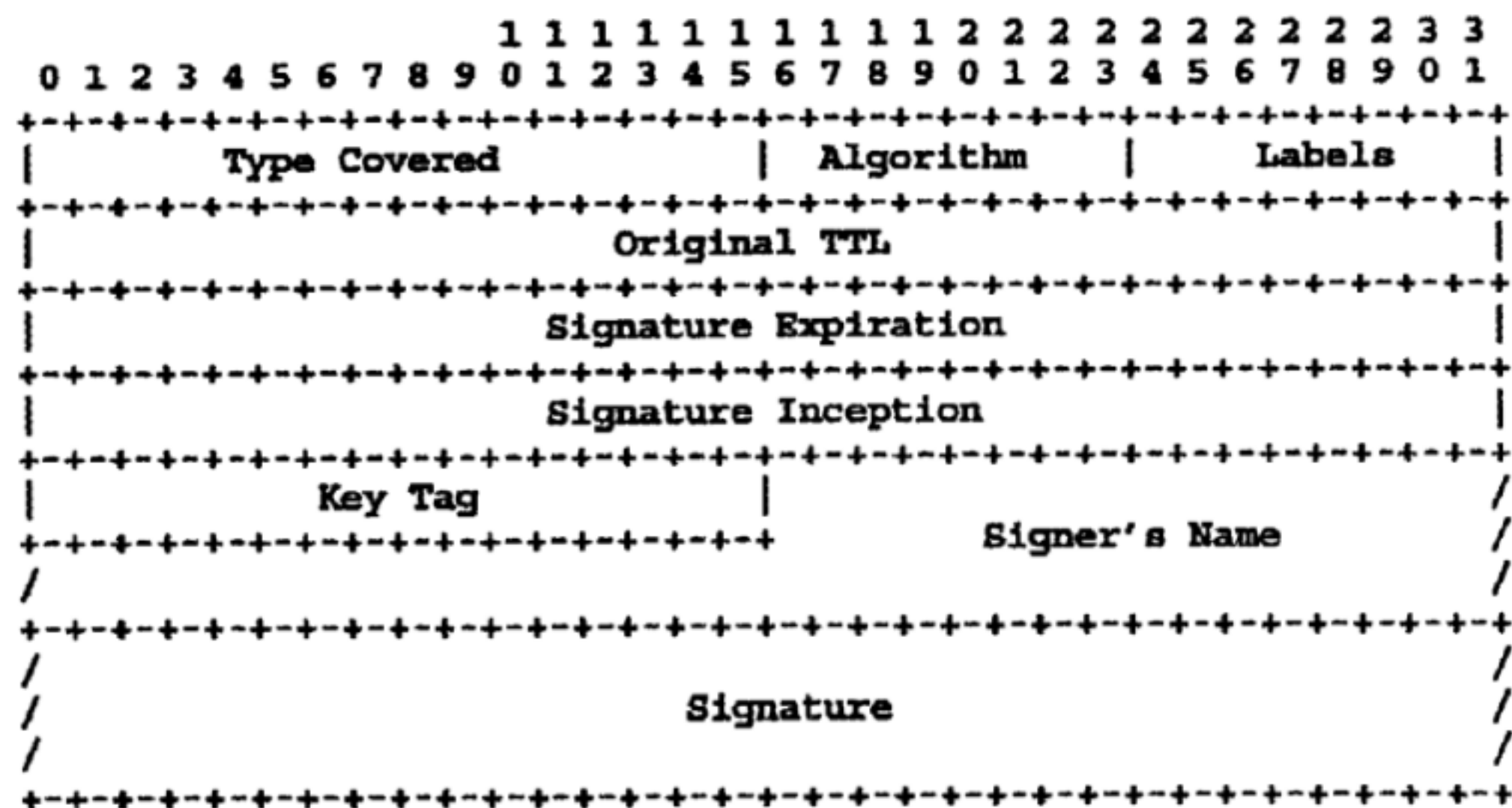


图2 RRSIG的报文格式

- 类型覆盖字段

类型覆盖字段指明该签名覆盖的资源记录的类型。

- 算法字段

算法字段指明该签名使用的是哪种数字签名算法。

- 域名字段

域名字段指明被签名的资源记录所有者中域名字段的数量，例如 `host.example.com` 为“3”，`*.example.com` 为 2，“.”的域名字段数量为“0”。

- 原始生命周期字段

原始生命周期字段指明该签名覆盖的资源记录集的生命周期。

- 签名过期时间字段和签名开始时间字段

签名过期时间字段和签名开始时间字段划定了签名的有效期。RRSIG 资源记录不能在签名开始时间之前使用，也不能在签名过期时间之后使用。

- 密钥标签字段

密钥标签字段是用对应的公钥数据简单叠加得到的一个 16 比特整数。如果一个权威域有多个密钥时，密钥标签可以和后面的签名者字段、算法字段共同帮助确定使用哪个公钥来验证签名（附录 D 给出了密钥标签字段计算方法的参考实例）。

- 签名者字段

签名者字段指明了签名覆盖的资源记录集的所有者。

- 签名字段

签名字段存储了资源记录集的数字签名，它的格式由所使用的签名算法决定。

5.3 NSEC3 资源记录

NSEC3 资源记录是为了应答那些不存在的资源记录而设计的。一个权威域的完整 NSEC3 资源记录链可以指明该权威域所有存在的资源记录类型及它们的所有者。NSEC3 与 NSEC 的区别在于：NSEC 中保存的是域名排序后的下一个域名的原始名称，而 NSEC3 保存的是域名的散列值。NSEC 所带来的安全问题是攻击者可以根据 NSEC 资源记录返回的内容推导出权威域中所有域名记录，而 NSEC3 中保存的是散列值，因此可以避免这种安全问题。

NSEC3 资源记录的类型值是 50。

NSEC3 资源记录的生命周期与 SOA 资源记录的最小生命周期值相同。

NSEC3 资源记录的报文格式如图 3 所示，包括 8 比特的散列算法字段（Hash Alg.）、8 比特的标志位（Flags）、16 比特的重复字段（Iterations）、8 比特的 Salt 长度字段（Salt Length）、Salt 字段（Salt）、8 比特的散列值长度字段（Hash Length）、下一个域名散列值字段（Next Hashed Owner Name）和类型位图字段（Type Bit Maps）。

- 散列算法字段

散列算法字段指明采用的哪种散列函数计算域名散列值。

- 标志位

除了最小的比特之外，标志位中其他比特均未定义，使用时需置零。

- 重复字段

重复字段表明散列函数重复使用的次数，即一个域名被散列函数重复计算的次数。它的值等于重复

计算的次数减一。

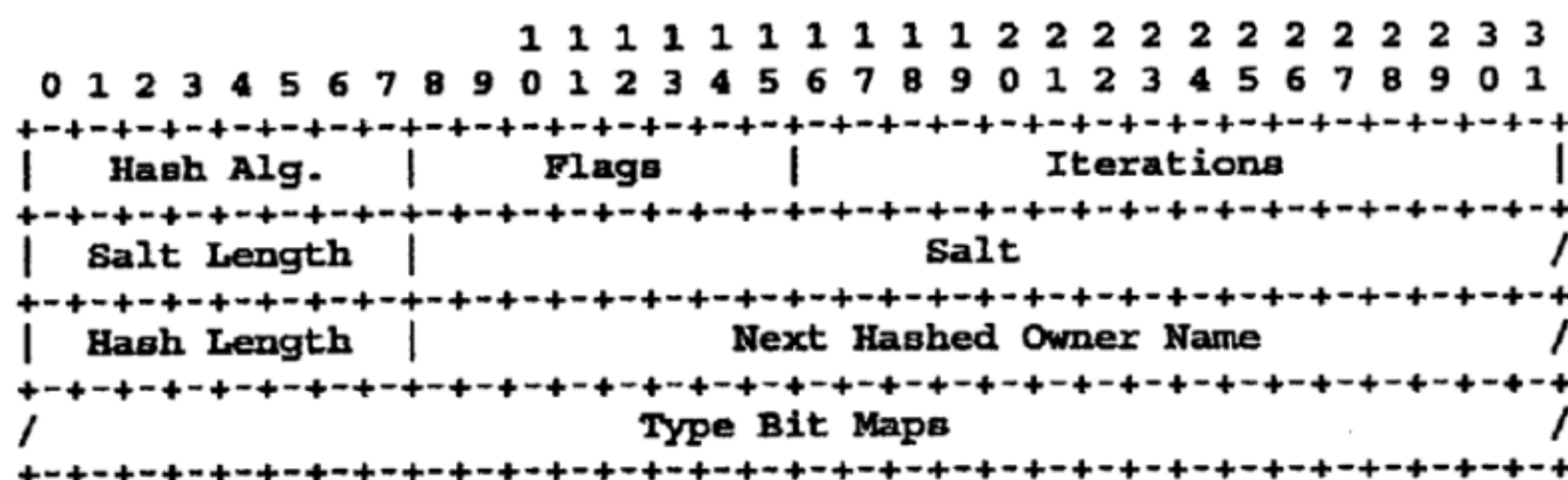


图3 NSEC3的报文格式

- Salt 长度字段

Salt 长度字段的值是 Salt 字段长度的十进制值，范围是 0~255。

- Salt 字段

Salt 字段用于计算域名的散列值。

- 散列值长度字段

散列值长度字段的值是下一个域名散列值字段长度的八进制值，范围是 1~255。

- 下一个域名散列值字段

下一个域名散列值字段指明权威域内的域名按照其散列值排序之后，下一个域名的散列值。

- 类型位图字段

类型位图字段指明 NSEC3 资源记录所有者拥有的全部资源记录类型。

5.4 DS 资源记录

DS 资源记录存储了 DNSKEY 资源记录的散列值，用于建立解析服务器验证 DNS 应答报文时所需的信任链，它可以验证与之对应的 DNSKEY 资源记录。DS 资源记录不像 DNSKEY 存储在资源记录所有者所在的权威域中，而是存储在上一级权威域中。

DS 资源记录的类型值是“43”。

DS 资源记录没有特殊的生命周期要求。

DS 资源记录的报文格式如图 4 所示，包括 16 比特的密钥标签字段（Key Tag）、8 比特的算法字段（Algorithm）、8 比特的散列类型字段（Digest Type）和散列值字段（Digest）。

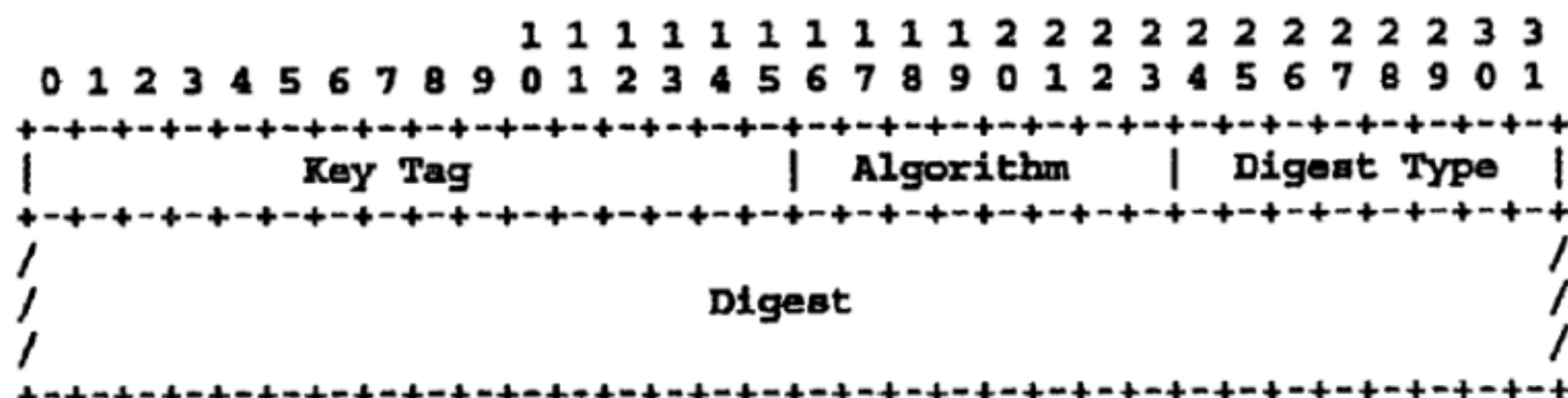


图4 DS的报文格式

- 密钥标签字段

DS 资源记录的密钥标签字段应和对应的 RRSIG 资源记录的密钥标签字段一致。

- 算法字段

算法字段和 DS 对应的 DNSKEY 资源记录的算法字段一致，表明签名所使用的算法种类。

- 散列类型字段

散列类型字段指明采用何种算法生成 DNSKEY 的散列值。

- 散列值字段

散列值字段存储 DNSKEY 的散列值。

6 DNSSEC 对 DNS 协议的修改

6.1 DNSSEC 对 DNS 报文的修改

由于新增的 DNSSEC 资源记录增加了 DNS 应答报文的长度，所以支持 DNSSEC 的权威域名服务器和解析服务器应支持 EDNS0，即 DNS 报文长度应最小支持 1220 字节，建议支持 4000 字节的报文。此外，DNSSEC 在报文头中增加了三个标志位：

(1) DO (DNSSEC OK)：支持 DNSSEC 的解析服务器在它的 DNS 查询报文中，应把 DO 标志位置“1”，否则权威域名服务器将认为解析服务器不支持 DNSSEC 就不会返回 RRSIG 等资源记录。

(2) AD (Authenticated Data)：AD 是已验证数据标志，如果解析服务器验证了 DNSSEC 应答报文中的数字签名，则置 AD 位为“1”，否则为“0”。这个标志位一般用于自己不做验证的解析服务器和它所信任的递归域名服务器之间，用户计算机上的解析服务器不验证数字签名，递归服务器给它一个 AD 标志为“1”的响应，它就接受验证结果。但是，这种场景应保证它们之间的通信链路安全，必要时需使用 IPSEC 和 TSIG。

(3) CD (Checking Disabled)：CD 是关闭检查标志，用于支持 DNSSEC 的解析服务器和递归域名服务器之间，解析服务器在发送请求时把 CD 位置“1”，递归域名服务器就不再进行数字签名的验证而把递归查询结果直接交给解析服务器，由解析服务器验证签名的合法性。

6.2 对 DNS 权威域名服务器的修改

支持 DNSSEC 的权威域名服务器应在给解析服务器的应答报文中包含适当的 DNSSEC 资源记录 (RRSIG、DNSKEY、DS 和 NSEC)，解析服务器通过查询报文中的 DO 标志位告知权威域名服务器自己希望接收哪些资源记录。但是新增的 DNSSEC 资源记录很容易导致应答报文超长，所以支持 DNSSEC 的权威域名服务器应支持 EDNS0。

支持 DNSSEC 的权威域名服务器应尽力将 RRSIG 资源记录 and 它覆盖的资源记录集放在同一个应答报文中发送。

支持 DNSSEC 的权威域名服务器在发送 DNSKEY、DS、NSEC 资源记录时应同时发送相应的 RRSIG 资源记录。

DNSSEC 资源记录应采用 Base64 编码方式。

DNSSEC 没有改变 DNS 的报文传输协议。

6.3 对 DNS 解析服务器的修改

支持 DNSSEC 的解析服务器应支持必要的加解密功能，以保证至少可以对使用某一种签名算法的数字签名进行认证。

支持 DNSSEC 的解析服务器应能够建立一个信任链，而且至少配置一个信任锚，作为信任链的起点。

支持 DNSSEC 的解析服务器对它所接收到的 RRSIG 资源记录，应能够区分以下四种结果：

(1) 安全的 (secure)：解析服务器能够建立到达资源记录签名者的信任链，并且可以验证数字签名的结果是正确的。

(2) 不安全的 (insecure)：解析服务器收到了一个资源记录和它的签名，但是它无法建立到达签名者的信任链，因而无法验证。

(3) 伪造的 (bogus)：解析服务器有一个到资源记录签名者的信任链，但是签名验证是错的。可能是因为受到攻击了，也可能是管理员配置错误。

(4) 不确定 (indeterminate)：解析服务器无法获得足够的 DNSSEC 资源记录，因而不能确定用户所请求的资源记录是否被签名。

6.4 如何验证 DNS 应答报文

为了验证一个支持 DNSSEC 的权威域名服务器发送的应答报文，支持 DNSSEC 的解析服务器应获得有效的 RRSIG 资源记录和对应的 DNSKEY 资源记录。解析服务器应建立信任链才能验证 DNSKEY 资源记录的真实性和完整性。成功验证 DNSKEY 以后，解析服务器才能够开始验证应答报文。在此，我们假设 DNSKEY 已经验证成功。

首先，解析服务器需要检验接收到的 RRSIG 资源记录是否有效。RRSIG 应满足如下条件：

- RRSIG 和它覆盖的资源记录集拥有相同的所有者；
- RRSIG 的签名者字段应是它覆盖的资源记录集的所有者；
- RRSIG 的类型覆盖字段应是它覆盖的资源记录集的类型；
- 资源记录集所有者的标签数量应大于或等于 RRSIG 的标签字段；
- 解析服务器的时间应小于 RRSIG 的签名过期时间字段；
- 解析服务器的时间应大于 RRSIG 的签名开始时间字段；
- RRSIG 的签名者字段、算法字段、密钥标签字段应与对应的 DNSKEY 一致。

之后，解析服务器重建原始的签名数据，包括 RRSIG 除签名字段以外的内容和它覆盖的资源记录集的规范形式。具体的重建格式参见 RFC 4035。

最后，解析服务器验证签名的合法性。签名保存在 RRSIG 的签名字段中，签名的公钥保存在 DNSKEY 的公钥字段中，RRSIG 的算法字段指明使用的签名算法。当验证成功之后，解析服务器需要设置验证过的资源记录集的生命周期，其值不能大于下列条件中的最小值：

- 接收到的资源记录集的生命周期；
- 接收到的 RRSIG 资源记录的生命周期；
- RRSIG 的原始生命周期字段；
- 解析服务器当前时间和 RRSIG 的签名过期时间字段的时间差。

7 DNSSEC 的部署实施要求

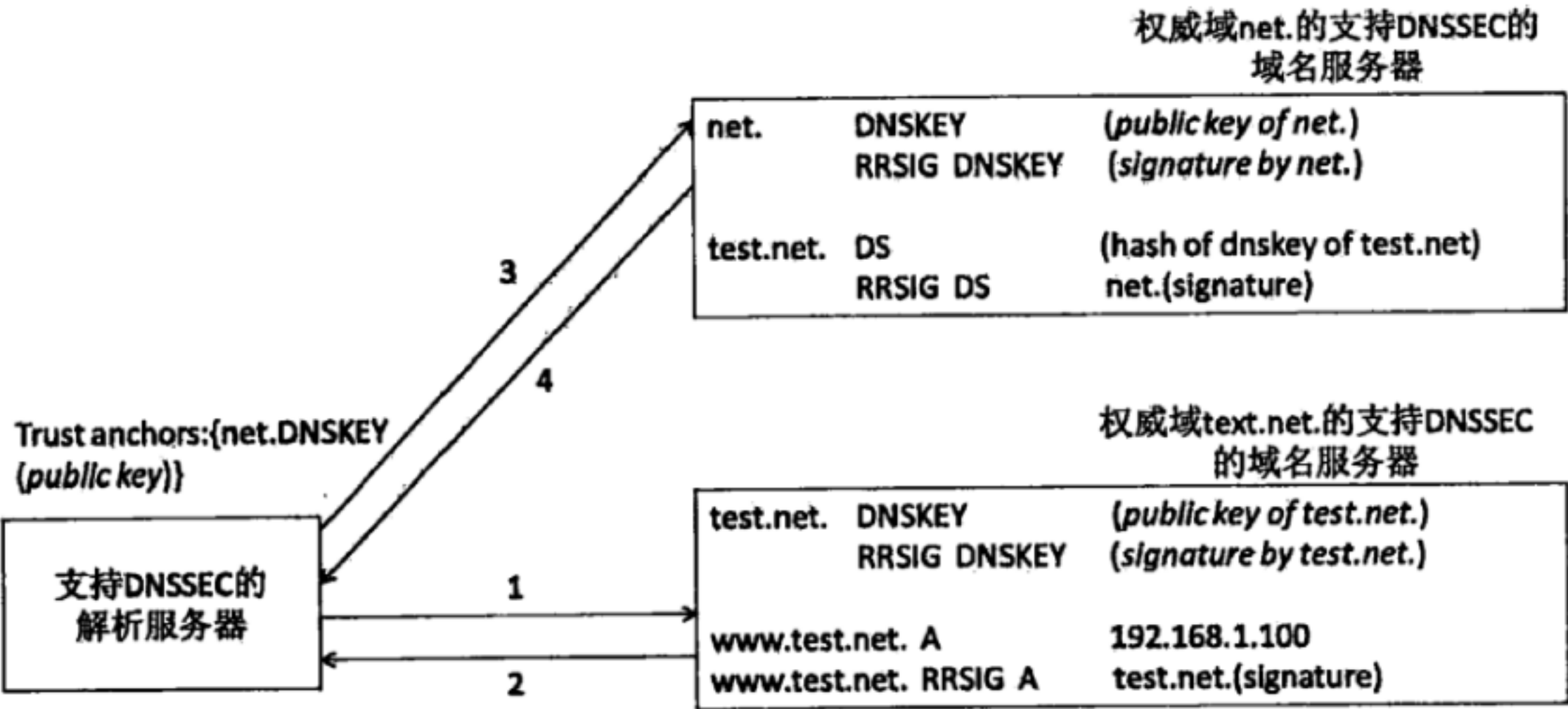
7.1 DNSSEC 的实施规范

相关要求见 YD/T 2140-2010，其中规定了支持 DNSSEC 的权威服务器和支持 DNSSEC 的递归服务器的实施要求。

附 录 A
(资料性附录)
DNSSEC原理举例说明

附录A通过一个简化的实例说明DNSSEC的工作原理。

如图A.1所示，一个支持DNSSEC的解析服务器向支持DNSSEC的权威域名服务器请求域名www.test.net.，它除了得到一个标准的A记录（包含IPv4地址）以外，还收到一个同名的RRSIG资源记录，其中包含test.net.权威域的数字签名，它是用test.net.的私钥来签名的。为了验证这一签名的合法性，解析服务器可以再次向test.net.权威域名服务器查询它的公钥，即名为test.net.的DNSKEY资源记录。然后解析服务器就可以使用这个公钥验证上述www.test.net. 记录的真实性与完整性。



图A.1 DNSSEC的原理

但是，解析服务器在得到 test.net.权威域的公钥之后，还需要认证该公钥的真实性。因此，DNSSEC需要一个信任链，而且应有一个或多个开始就被信任的公钥（或公钥的散列值）作为信任链的起点。信任链中的上一个节点为下一个节点的公钥散列值进行数字签名，从而保证信任链中的每一个公钥都是真实的。理想的情况下（DNSSEC 全部部署），每个解析服务器只需要保存根域名服务器的 DNSKEY 资源记录作为信任锚就可以建立起能够到达任意权威域的信任链。

在上面的例子中，假设解析服务器开始并不信任test.net.的公钥，它可以到test.net.的上一级权威域名服务器net.那里查询test.net.的DS（Delegation Signer）资源记录，DS资源记录中存储的是test.net.公钥的散列值。假设解析服务器由管理员手工配置了.net的公钥（即信任锚），它就可以验证test.net.公钥（DNSKEY 资源记录）的真实与否了。

附 录 B
(资料性附录)
DNSSEC国际部署情况

附录B为DNSSEC的国际部署情况，如下：

a) .SE (瑞典) 早在2001年就启动DNSSEC项目，2005年9月完成对.SE区签名，2007年2月16日进行商业运行；.SE是国际上第一个完成DNSSEC部署的顶级域，对全球产生非常大的影响，此后其他国家(地区)开始陆续实施DNSSEC。

b) .ORG 在 2009 年 6 月 2 日 正 式 完 成 DNSSEC 部 署；DNSSEC 所用 密 钥 算 法 为：RSASHA1-NSEC3-SHA1，使用NSEC3PARAM签名；密钥长度KSK采用2048位，ZSK采用1024位。

c) 2010年1月份，在L根上部署完DNSSEC，状态为DURZ；2010年5月份旬，所有的根服务器部署完DNSSEC。

d) 2010年7月15日，ICANN公布DNSSEC信任锚点，根区正式向互联网提供DNSSEC服务。

e) 2010年11月4日，美国Verisign公司完成.NET域名DNSSEC的实施；DNSSEC所用密钥算法为RSA/SHA-256，使用NSEC3PARAM签名；密钥长度KSK采用2048位，ZSK采用1024位。

f) 2011年3月2日，全球注册量最大顶级域.COM开始部署DNSSEC，但签名密钥均为测试密钥，处于部署、试运行状态。

g) 2011年3月21日，Verisign向根区提交.COM 的DS记录，并向互联网公布.COM提供DNSSEC解析验证服务。

h) 2011年3月2日，全球注册量最大顶级域.COM开始部署DNSSEC，但签名密钥均为测试密钥，处于部署、试运行状态。

i) 2011年3月21日，Verisign向根区提交.COM 的DS记录，并向互联网公布.COM提供DNSSEC解析验证服务。

j) 截至2011年7月18日，已完成DNSSEC部署的顶级域共有73个，其中ccTLD有50个，gTLD有11个，IDN有13个。

附 录 C
(资料性附录)
DNSSEC实例

附录C为DNSSEC实例。

一个完整的支持DNSSEC的权威域记录文件范例如下：

```
example.      3600 IN SOA   ns1.example. bugs.x.w.example. (
                                1081539377
                                3600
                                300
                                3600000
                                3600
                                )
              3600 RRSIG  SOA 5 1 3600 20040509183619 (
                                20040409183619 38519 example.
                                ONx0k36rcjaxYtcNgq6iQnpNV5+drqYAsC9h
                                7TSJaHCqbhE67Sr6aH2xDUGcqQWu/n0UVzrF
                                vkgO9ebarZ0GWDKcuwlM6eNB5SiX2K74l5LW
                                DA7S/Un/IbtDq4Ay8NMNLQI7Dw7n4p8/rkB
                                jV7j86HyQgM5e7+miRAz8V01b0I= )
              3600 NS     ns1.example.
              3600 NS     ns2.example.
              3600 RRSIG  NS 5 1 3600 20040509183619 (
                                20040409183619 38519 example.
                                gl13F00f2U0R+SWiXXLHwsMY+qStYy5k6zfd
                                EuivWc+wd1fmbNCyql0Tk7lHTX6UOxc8AgNf
                                4ISFve8XqF4q+o9qlnqlzmppU3LiNeKT4FZ8
                                RO5urFOvoMRTbQxW3U0hXWuggE4g3ZpsHv48
                                0HjMeRaZB/FRPGfJPajngcq6Kwg= )
              3600 MX     1 xx.example.
              3600 RRSIG  MX 5 1 3600 20040509183619 (
                                20040409183619 38519 example.
                                HyDHYVT5KHSZ7HtO/vypumPmSZQrcOP3tzWB
                                2qaKkHVPfau/DgLgS/IKENkYOGl95G4N+NzE
                                VyNU8dcTOckT+ChPcGeVjguQ7a3Ao9Z/ZkUO
                                6gmmUW4b89rz1PUxW4jzUxj66PTwoVtUU/iM
                                W6OISukd1EQt7a0kygkg+PEDxdI= )
```

3600 NSEC	a.example. NS SOA MX RRSIG NSEC DNSKEY
3600 RRSIG	NSEC 5 1 3600 20040509183619 (20040409183619 38519 example. O0k558jHhyrC97ISHnism4kLMW48C7U7cBm FTfhke5iVqNRVTB1STLMpgpbDIC9hcryoO0V Z9ME5xPzUEhbnGnHd5sfzgFVeGxr5Nyyq4tW SDBgIBiLQUv1ivy29vhXy7WgR62dPrZ0PWvm jfFJ5arXf4nPxp/kEowGgBRzY/U=)
3600 DNSKEY	256 3 5 (AQOy1bZVvpPqhg4j7EJoM9rI3ZmyEx2OzDBV rZy/lvI5CQePxXHZS4i8dANH4DX3tbHol61e k8EFMcsGXxKciJFHyhl94C+NwILQdzsUlsFo vBZsyl/NX6yEbtw/xN9ZNcrbYvgjjZ/UVpZI ySFNsgEYvh0z2542lzMKR4Dh8uZffQ=)
3600 DNSKEY	257 3 5 (AQOeX7+baTmvpVHb2CcLnL1dMRWbuscRvHXl LnXwDzvqp4tZVKp1sZMepFb8MvxhhW3y/0QZ syCjczGJ1qk8vJe52iOhInKROVLRwxGpMfzP RLMlGybr51bOV/1se0ODacj3DomyB4QB5gKT Yot/K9alk5/j8vfd4jWCWD+E1Sze0Q=)
3600 RRSIG	DNSKEY 5 1 3600 20040509183619 (20040409183619 9465 example. ZxgauAulj+k1YoVEOSlZfx4lfcMkzTFHoweZ xYnz99JVQZJ33wFS0Q0jcP7VXKkaElXk9nYJ XevO/7nAbo88iWsMkSpSR6jWzYYKwfrBI/L9 hjYmyVO9m6FjQ7uwM4dCP/bIuV/DKqOAK9NY NC3AHfvCV1Tp4VKDqxqG7R5tTVM=)
3600 RRSIG	DNSKEY 5 1 3600 20040509183619 (20040409183619 38519 example. eGL0s90glUqcOml00/2y+bSzyEfKVOQViD9Z DNhLz/Yn9CQZlDVRJffACQDAUhXpU/oP34ri bKBpysRXosczFrKqS5Oa0bzMOFXCXup9qHAp eFlku28Vqfr8Nt7cigZLxjK+u0Ws/4lIRjKk 7z5OXogYVaFzHKillDt3HRxHIZM=)
a.example.	3600 IN NS ns1.a.example.

	3600 IN NS	ns2.a.example.
	3600 DS	57855 5 1 (B6DCD485719ADCA18E5F3D48A2331627FDD3 636B)
	3600 RRSIG	DS 5 2 3600 20040509183619 (20040409183619 38519 example. oXIKit/QtdG64J/CB+Gi8dOvnwRvqrto1AdQ oRkAN15FP3iZ7suB7gvTBmXzCjL7XUgQVcoH kdhyCuzp8W9qJHgRUSwKKkczSyuL64nhgjuD EML8l9wlWVsl7PR2VnZduM9bLyBhaaPmRKX/ Fm+v6ccF2EGNLRiY08kdkz+XHHo=)
	3600 NSEC	ai.example. NS DS RRSIG NSEC
	3600 RRSIG	NSEC 5 2 3600 20040509183619 (20040409183619 38519 example. cOlYgqJLqlRqmBQ3iap2SyIsK4O5aqpKSoba U9fQ5SMApZmHfq3AgLflkrkXRXvgxTQSKkG2 039/cRU6Jk/25+fi7Xr5nOVJsb0lq4zsB3I BBdjyGDAHE0F5ROJj87996vJupdm1fbH481g sdkOW6Zyqtz3Zos8N0BBkEx+2G4=)
ns1.a.example.	3600 IN A	192.0.2.5
ns2.a.example.	3600 IN A	192.0.2.6
ai.example.	3600 IN A	192.0.2.9
	3600 RRSIG	A 5 2 3600 20040509183619 (20040409183619 38519 example. pAOtzLP2MU0tDJUwHOKE5FPIIHmdYsCgTb5B ERGgpnJluA9ixOyf6xxVCgrEJW0WNZSsJicd hBHxfDmAGKUajUUIYSAH8tS4ZnrhyymIvk3u ArDu2wftT130e9UHnumaHHMpUTosKe22PblOy 6zrTpg9FkS0XGVmYRvOTNYx2HvQ=)
	3600 HINFO	"KLH-10" "ITS"
	3600 RRSIG	HINFO 5 2 3600 20040509183619 (20040409183619 38519 example. Iq/RGCBdKzcYzlGE4ovbr5YcB+ezxbZ9W0l e/7WqyvhhOO9J16HxhhL7VY/IKmTUY0GGdcfh ZEOckf4lEyKZF9NPok1/R/fWrtzNp8jobuY7 AZEczadp1WdDF3jc2/ndCa5XZhLKD3JzOsBw FvL8sqlS5QS6FY/ijFEDnI4RkZA=)

3600 AAAA	2001:db8::f00:baa9
3600 RRSIG	AAAA 5 2 3600 20040509183619 (20040409183619 38519 example. nLcpFuXdT35AcE+EoafOUkl69KB+/e56XmFK kewXG2IadYLKAOBIO5+VoQV3XgTcofTJNsh 1rnF6Eav2zpZB3byI6yo2bwY8MNkr4A7cL9T cMmDwV/hWFKsbGBsj8xSCN/caEL2CWY/5XP2 sZM6QjBBLmukH30+w1z3h8PUP2o=)
3600 NSEC	b.example. A HINFO AAAA RRSIG NSEC
3600 RRSIG	NSEC 5 2 3600 20040509183619 (20040409183619 38519 example. QoshyPevLcJ/xcRpEtMft1uoIrcieVcc9pG CScIn5Glnib40T6ayVOimXwdSTZ/8ISXGj4p P8Sh0PIA6olZQ84L453/BUqB8BpdOGky4hsN 3AGcLEv1Gr0QMvirQaFcjzOECfnGyBm+wpFL AhS+JOVfDI/79QtyTI0SaDWcg8U=)
b.example. 3600 IN NS	ns1.b.example.
3600 IN NS	ns2.b.example.
3600 NSEC	ns1.example. NS RRSIG NSEC
3600 RRSIG	NSEC 5 2 3600 20040509183619 (20040409183619 38519 example. GNuxHn844wfmUhPzGWKJCPY5ttEX/RfjDoOx 9ueK1PtYkOWKOOdiJ/PJKCYB3hYX+858dDWS xb2qnV/LSTCNVBnkm6owOpysY97MVj5VQEWs 0lm9tFoqjcptQkmQKYPrwUnCSNwvvelSF1xZ vhRXgWT7OuFXldoCG6TfVFM9xE=)
ns1.b.example. 3600 IN A	192.0.2.7
ns2.b.example. 3600 IN A	192.0.2.8
ns1.example. 3600 IN A	192.0.2.1
3600 RRSIG	A 5 2 3600 20040509183619 (20040409183619 38519 example. F1C9HVhIcs10cZU09G5yIVfKJy5yRQQ3qVet 5pGhp82pzhAOMZ3K22JnmK4c+IjUeFp/to06 im5FVpHtbFisdjyPq84bhTv8vrXt5AB1wNB+ +iAqvIfdgW4sFNC6oADb1hK8QNauw9VePJhK v/iVXSYC0b7mPSU+E0lknFpVECs=)
3600 NSEC	ns2.example. A RRSIG NSEC

3600 RRSIG	NSEC 5 2 3600 20040509183619 (20040409183619 38519 example. I4hj+Kt6+8rCcHcUdolks2S+Wzri9h3fHas8 1rGN/eILdJHN7JpV6ILGPIh/8fIBkfvdyWnB jiflq3O7JgYO1UdI7FvBNWqaaEPJK3UkddBq ZlaLi8Qr2XHkj38BeQsbp8X0+6h4ETWSGT8 IZaIGBLryQWGLw6Y6X8dqhlxJM=)
ns2.example. 3600 IN A	192.0.2.2
3600 RRSIG	A 5 2 3600 20040509183619 (20040409183619 38519 example. V7cQRw1TR+knlaL1z/psxlS1PcD37JJDaCMq Qo6/u1qFQu6x+wuDHRH22Ap9ulJPQjFwMKOu yfPGQPC8KzGdE3vt5snFEAoE1Vn3mQqtu7SO 6amljk13Kj/jyJ4nGmdRIc/3cM3ipXFhNTKq rdhx8SZ0yy4ObIRzIzvBFLiSS8o=)
3600 NSEC	*.w.example. A RRSIG NSEC
3600 RRSIG	NSEC 5 2 3600 20040509183619 (20040409183619 38519 example. N0QzHvaJf5NRw1rE9uxS1Ltb2LZ73Qb9bKGE VyaISkqzGpP3jYJXZJPVTq4UVEsgT3CgeHvb 3QbeJ5Dfb2V9NGCHj/OvF/LBxFFWwhLwzngH l+bQAgAcMsLu/nL3nDily/JSQjAcdZNDl4bw Ymx28EtgIpo9A0qmP08rMBqs1Jw=)
*.w.example. 3600 IN MX	1 ai.example.
3600 RRSIG	MX 5 2 3600 20040509183619 (20040409183619 38519 example. OMK8rAZlepflLWW75Dxd63jy2wswESzxDKG2 f9AMN1CytCd10cYISAxAdvXSZ7xujKAtPbc tvOQ2ofO7AZJ+d01EeeQTVBPq4/6KCWhqe2X TjnkVLNvvhnc0u28aoSsG0+4InvkkOHknKxw 4kX18MMR34i8lC36SR5xBni8vHI=)
3600 NSEC	x.w.example. MX RRSIG NSEC
3600 RRSIG	NSEC 5 2 3600 20040509183619 (20040409183619 38519 example. r/mZnRC3I/VlcrelIcteSxDhtsdlTDt8ng9 HSBlABOlzLxQtfgTnn8f+aOwJIAFe1Ee5RvU 5cVhQJNP5XpXMJHfyps8tVvfxSAXfahpYqtx

		91gsmcV/1V9/bZAG55CefP9cM4Z9Y9NT9XQ8 s1InQ2UoIv6tJEaaKkP701j8OLA=)
x.w.example.	3600 IN MX	1 xx.example.
	3600 RRSIG	MX 5 3 3600 20040509183619 (20040409183619 38519 example. Il2WTZ+Bkv+OytBx4LItnW5mjB4RCwhOO8y1 XzPHZmZUTVYL7LaA63f6T9ysVBzJRI3KRjAP H3U1qaYnDoN1DrWqmi9RJe4FoObkbcdm7P3I kx70ePCoFgRz1Yq+bVVXCvGuAU4xALv3W/Y1 jNSlwZ2mSWKHfXQxPtLj8s32+k=)
	3600 NSEC	x.y.w.example. MX RRSIG NSEC
	3600 RRSIG	NSEC 5 3 3600 20040509183619 (20040409183619 38519 example. aRbpHftxggzgMXdDlym9SsADqMZovZZI2QWK vw8J0tZEUNQByH5Qmf5N1FqH/pS46UA7A4E mcWBN9PUA1pdPY6RVearlZlCr1IkVctvbtal NJUBba/VHm+pebTbKcAPIvL9tBOoh+tolh6e IjgiM8PXkBQtxPq37wDKALkyn7Q=)
x.y.w.example.	3600 IN MX	1 xx.example.
	3600 RRSIG	MX 5 4 3600 20040509183619 (20040409183619 38519 example. k2bJHbwP5LH5qN4is39UiPzjAWYmJA38Hhia t7i9t7nbX/e0FPnvDSQXzcK7UL+zrVA+3MDj q1ub4q3SZgcbLMgexxIW3Va//LVrxkP6Xupq GtOB9prkK54QTL/qZTXfMQpW480YOvVknhvb +gLcMZBnHJ326nb/TOOmqrNmQQE=)
	3600 NSEC	xx.example. MX RRSIG NSEC
	3600 RRSIG	NSEC 5 4 3600 20040509183619 (20040409183619 38519 example. OvE6WUzN2ziieJcvKPWbCAyXyP6ef8cr6Csp ArVSTzKSquNwbezZmkU7E34o5lmb6CWSSSpG xw098kNUFnHcQf/LzY2zqRomubrNQhJTIDTX a0ArunJQCzPjOYq5t0SLjm6qp6McJI1AP5Vr QoKqJDCLnoAlcPOPkAm/jJkn3jk=)
xx.example.	3600 IN A	192.0.2.10
	3600 RRSIG	A 5 2 3600 20040509183619 (20040409183619 38519 example.

```

kBF4YxMGWF0D8r0cztL+2fWWOvN1U/GYSpYP
7SoKoNQ4fZKyK+weWGikLIUM+uE1zjVTPXoa
0Z6WG0oZp46rkl1EzMcdMgoaeUzzAJ2BMq+Y
VdxG9IK1yZkYGY9AgbTOGPoAgbJyO9EPULsx
kbIDV6GPPSZVusnZU6OMgdgzHV4= )

3600 HINFO "KLH-10" "TOPS-20"
3600 RRSIG HINFO 5 2 3600 20040509183619 (
20040409183619 38519 example.
GY2PLSXmMHkWHfLdggiox8+chWpeMNJLkML0
t+U/SXSUsoUdR91KNdNUkTDWamwcF8oFRjhq
BcPZ6EqrF+vl5v5oGuvSF7U52epfVTC+wWF8
3yCUeUw8YklhLWlvk8gQ15YKth0ITQy8/wI+
RgNvuwbioFSEuv2pNlkq0goYxNY= )

3600 AAAA 2001:db8::f00:baaa
3600 RRSIG AAAA 5 2 3600 20040509183619 (
20040409183619 38519 example.
Zzj0yodDxcBLnnOIwDsuKo5WqiaK24DlKg9C
aGaxDFiKgKobUj2jilYQHpGFn2poFRetZd4z
ulyQkssz2QHrVrPuTMS22knudCiwP4LWpVTr
U4zfeA+rDz9stmSBP/4PekH/x2IoAYnwctd/
xS9cL2QgW7FChw16mzlkH6/vsfs= )

3600 NSEC example. A HINFO AAAA RRSIG NSEC
3600 RRSIG NSEC 5 2 3600 20040509183619 (
20040409183619 38519 example.
ZFWUln6Avc8bmGl5GFjD3BwT530DUZKHNUoY
9A8lgXYyrxu+pqgFiRVbyZRQvVB5pccEOT3k
mvHgEa/HzbDB4PIYY79W+VHrgOxzdQGGCZzi
asXrpSGOWwSOElghPnMli8xdF7qtCntr382W
GghLahumFIpg4MO3LS/prgzVWwo= )

```

在这个权威域中有两个DNSKEY资源记录，一个是区签名密钥，一个是密钥签名密钥。同时，这个权威域包括了两个代表点，指向b.example的代表点包括了域名服务器（NS）资源记录、胶水地址记录和NSEC资源记录，其中只有NSEC被签名；指向a.example的代表点除了上述记录外，还包括了DS资源记录，其中只有DS和NSEC被签名。

下面是一个DNSSEC应答消息的实例，其中的数据引自上述权威域实例。

```

;; 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. Il2WTZ+Bkv+OytBx4LItNW5mjB4RCwhOO8y1 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. gl13F00f2U0R+SWiXXLHwsMY+qStYy5k6zfd EuivWc+wd1fmbNCyql0Tk7lHTX6UOxc8AgNf 4ISFve8XqF4q+o9qlnqlzmppU3LiNeKT4FZ8 RO5urFOvoMRTbQxW3U0hXWuggE4g3ZpsHv48 0HjMeRaZB/FRPGfJPajngcq6Kwg=)
;; 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+weWGIKLlUM+uE1zjVTPXoa 0Z6WG0oZp46rk1lEzMcdMgoaeUzzAJ2BMq+Y VdxG9IK1yZkYGY9AgbTOGPoAgbJyO9EPULsx 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=)

YD/T 2586-2013

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+EOlknFpVECs=)
ns2.example.	3600 IN A	192.0.2.2
ns2.example.	3600 RRSIG	A 5 2 3600 20040509183619 (20040409183619 38519 example. V7cQRw1TR+knlaL1z/psxlS1PcD37JJDaCMq Qo6/u1qFQu6x+wuDHRH22Ap9ulJPQjFwMKOu yfPGQPC8KzGdE3vt5snFEAoE1Vn3mQqtu7SO 6amIjk13Kj/jyJ4nGmdRIc/3cM3ipXFhNTKq rdhx8SZ0yy4ObIRzIzvBFLiSS8o=)

附 录 D
(资料性附录)
密钥标签字段计算方法

附录D为RRSIG的密钥标签字段的计算方法及实现实例。

RRSIG和DS资源记录中的密钥标签字段提供了一种有效地识别权威域公钥的方法，它与RRSIG资源记录中的签名者字段、算法字段能够共同帮助确定使用哪一个权威域公钥来验证签名。但是，不能排除存在相同密钥标签字段、签名者字段和算法字段的两个不同公钥的情况，因此密钥标签字段不能够唯一确定应该使用哪个权威域公钥。

下面是一个用C语言实现的计算密钥标签字段数值的参考实例，输入项是DNSKEY资源记录数据的线性格式。

```
/*
 * Assumes that int is at least 16 bits.
 * First octet of the key tag is the most significant 8 bits of the
 * return value;
 * Second octet of the key tag is the least significant 8 bits of the
 * return value.
 */
unsigned int
keytag (
    unsigned char key[],      /* the RDATA part of the DNSKEY RR */
    unsigned int keysize     /* the RDLENGTH */
)
{
    unsigned long ac;         /* assumed to be 32 bits or larger */
    int i;                   /* loop index */
    for ( ac = 0, i = 0; i < keysize; ++i )
        ac += (i & 1) ? key[i] : key[i] << 8;
    ac += (ac >> 16) & 0xFFFF;
    return ac & 0xFFFF;
}
```

参 考 文 献

1. IETF RFC 4033 DNSSEC的介绍和需求
 2. IETF RFC 4034 资源记录支持DNSSEC的扩展
 3. IETF RFC 4035 支持DNSSEC的协议修改
 4. IETF RFC 5155 散列的DNSSEC否定存在验证
-

中 华 人 民 共 和 国
通 信 行 业 标 准
域名服务系统安全扩展（DNSSEC）协议和实现要求
YD/T 2586-2013

*

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：100064
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2013 年 12 月第 1 版
印张：1.75 2013 年 12 月北京第 1 次印刷
字数：46 千字

15115 • 329

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492