DNSSEC如何保障域名解析安全

——技术原理和安全特性

Concepts, deployment & security implications of DNSSEC

陆超逸

清华大学 网络科学与网络空间研究院 博士后

2023年5月25日

问卷调查

我们希望了解您对于DNSSEC协议的看法
烦请填写下面的问卷调查

感谢您为推动DNSSEC部署和提升校园网安全作出的贡献！

关于校园网DNSSEC部署应用现状的调查问卷

尊敬的先生/女士:

您好！没有网络安全就没有国家安全，网络安全也是学校信息化的基本保障和底线。为了提高校园网信息化的安全水平，我们特意开展校园信息化安全状况调研和前沿安全技术及解决方案的调研。鉴于贵校在网络安全方面取得的学术成就和影响，特邀请贵校参与此次调研，希望得到您的大力支持。

问卷链接：https://www.wjx.cn/vm/tGgi4jB.aspx#

可扫描二维码
填写问卷

主要内容

一、DNSSEC
能解决什么问题

二、DNSSEC的
工作原理

三、DNSSEC的
部署应用现状

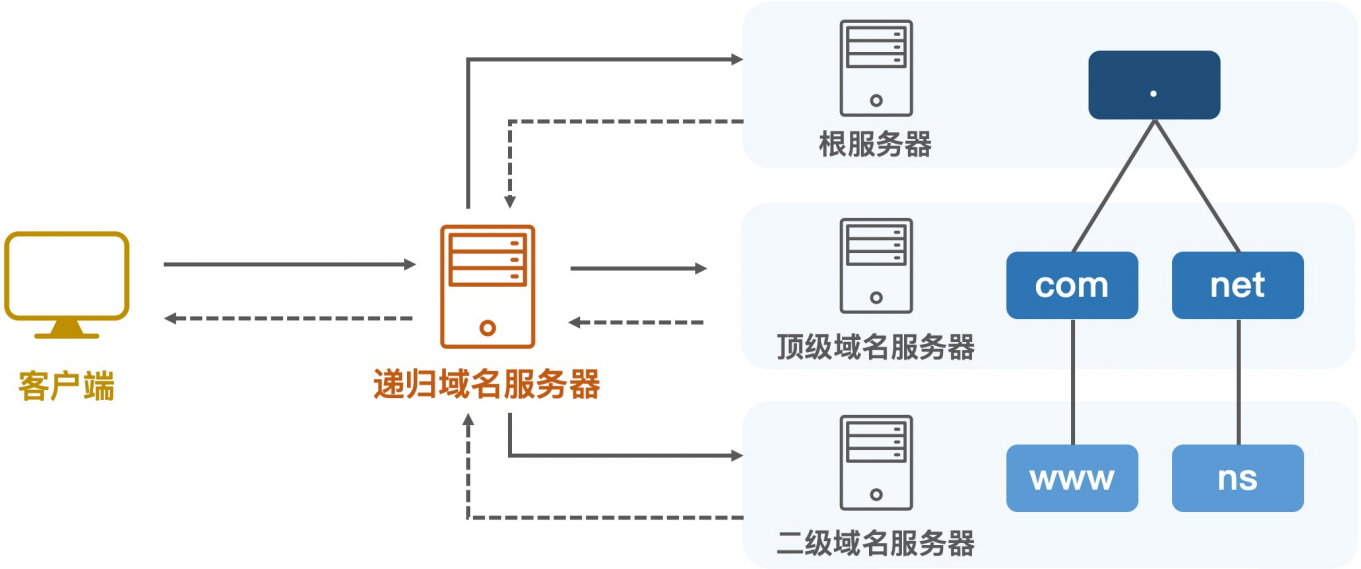
四、DNSSEC的
配置注意事项

第一部分　Part I

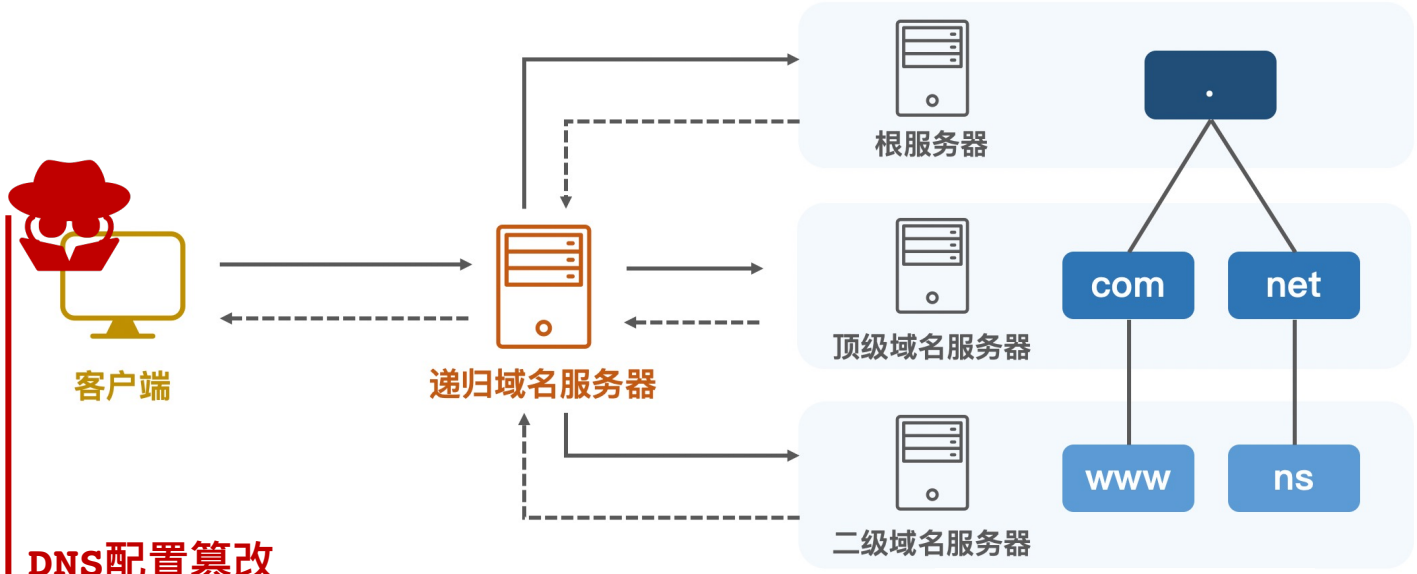
DNSSEC能解决什么问题

域名解析面临什么样的威胁?

攻击者可能出现在什么位置?



域名解析面临什么样的威胁?



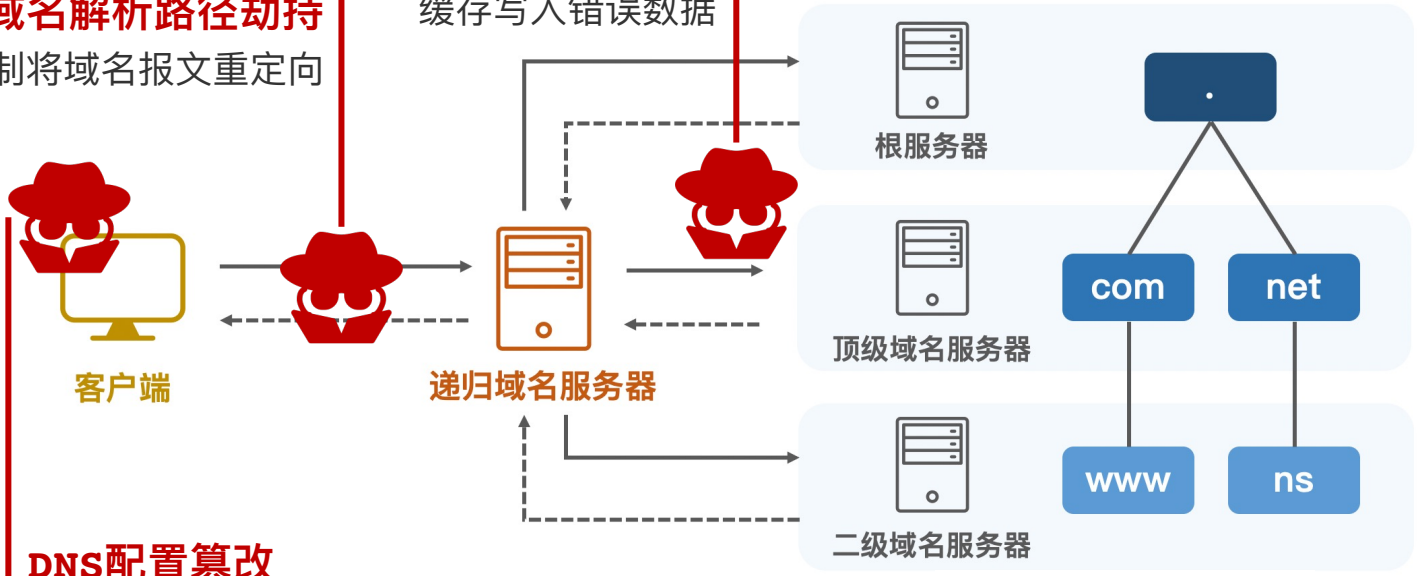
DNS配置篡改

通过恶意软件修改操作系统的DNS配置

域名解析面临什么样的威胁？

中间人域名劫持
篡改响应报文
域名解析路径劫持
强制将域名报文重定向

缓存污染攻击
向递归域名服务器的
缓存写入错误数据



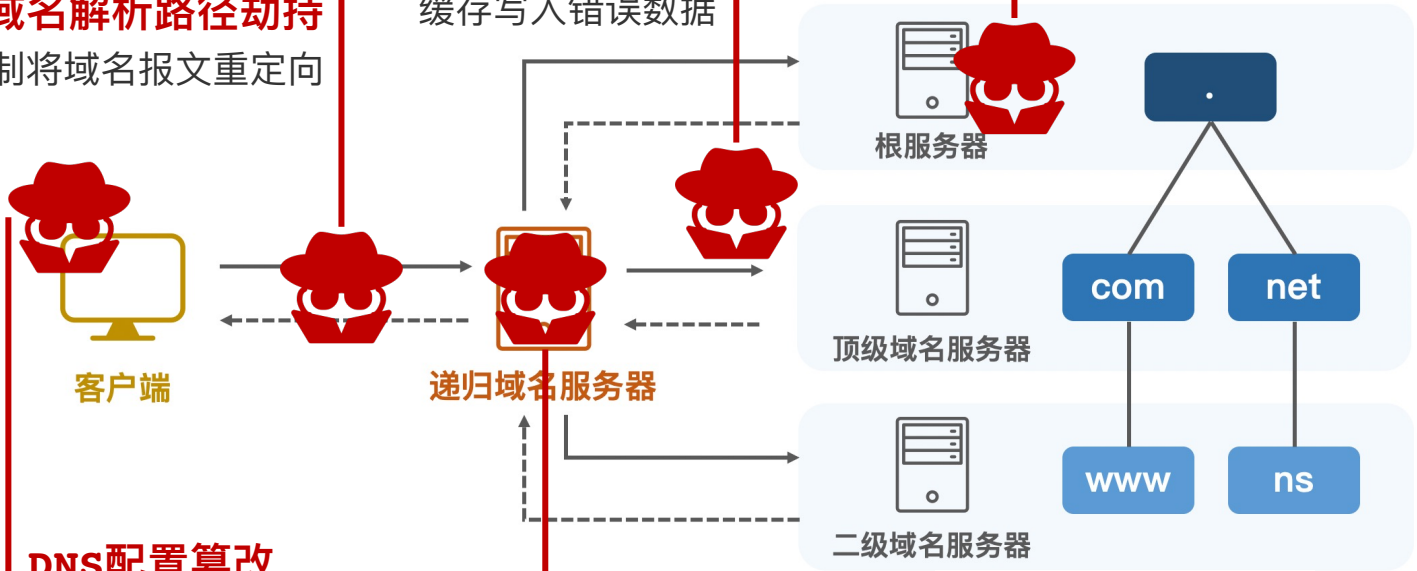
DNS配置篡改
通过恶意软件修改操作
系统的DNS配置

域名解析面临什么样的威胁？

中间人域名劫持
篡改响应报文
域名解析路径劫持
强制将域名报文重定向

缓存污染攻击
向递归域名服务器的
缓存写入错误数据

恶意/虚假权威服务器
非授权的服务器镜像



DNS配置篡改
通过恶意软件修改操作
系统的DNS配置

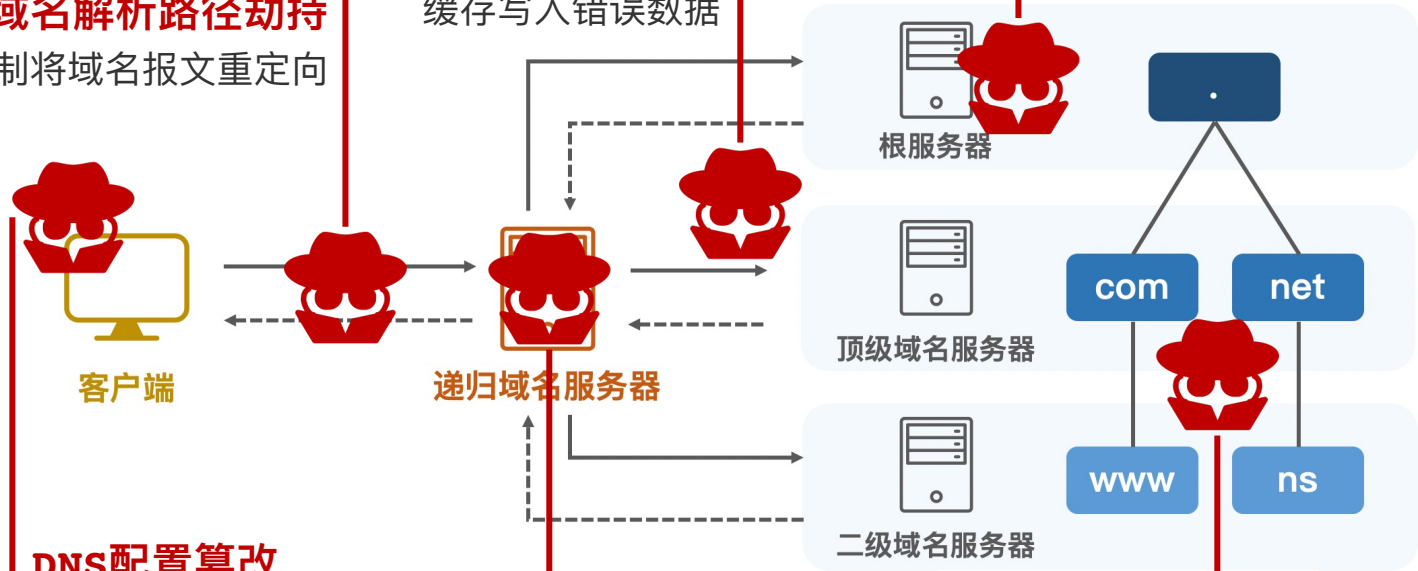
恶意域名服务器
故意返回错误的解析结果

域名解析面临什么样的威胁？

中间人域名劫持
篡改响应报文
域名解析路径劫持
强制将域名报文重定向

缓存污染攻击
向递归域名服务器的
缓存写入错误数据

恶意/虚假权威服务器
非授权的服务器镜像



DNS配置篡改
通过恶意软件修改操作
系统的DNS配置

恶意域名服务器
故意返回错误的解析结果

域名滥用
将域名用于恶意行为

“打补丁”式的安全防御思路

上述安全问题，由域名系统的哪些缺陷引起?

缺什么，我们就加什么

缺陷	安全风险	典型案例
消息完整性缺失	无法校验响应是否被篡改	中间人域名劫持 旁路注入攻击（缓存污染） 恶意域名服务器
身份认证机制缺失	无法校验解析报文的来源	域名解析路径劫持攻击 恶意域名服务器 拒绝服务攻击（DoS）
消息保密性缺失	解析报文对链路设备可见	用户隐私嗅探

“打补丁”式的安全防御思路

上述安全问题，由域名系统的哪些缺陷引起?

缺什么，我们就加什么

缺陷	解决方案
消息完整性缺失	**域名签名协议（DNSSEC）** 对资源记录进行**数字签名和验证，避免响应报文被恶意篡改**
身份认证机制缺失	**加密域名协议（Encrypted DNS，此次不涉及）** 使用**加密信道**传输域名解析报文，基于证书进行身份认证
消息保密性缺失	

第二部分　Part II

DNSSEC的工作原理

DNSSEC的工作原理：概述

数字签名（Digital signature）：发送方签名、接收方验证

发送方使用**私钥签名**、公开公钥，接收方使用**公钥验证**

私钥只有发送方拥有 -> 数字签名无法伪造

DNSSEC的工作原理：概述

数字签名（Digital signature）：发送方签名、接收方验证

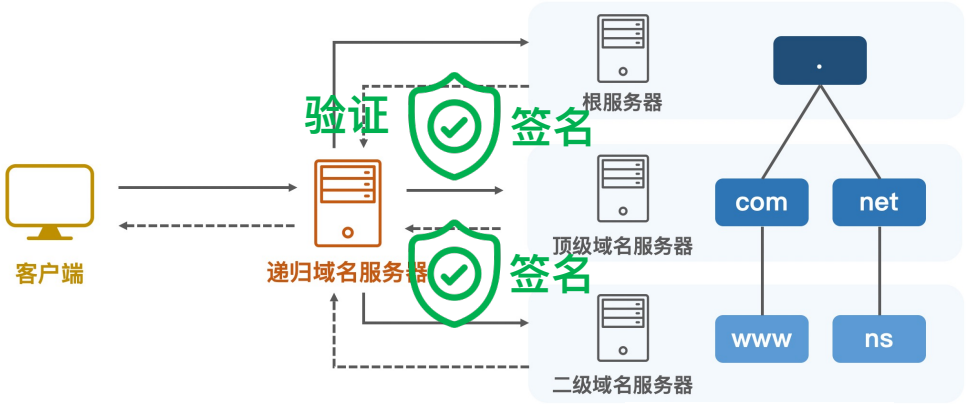
发送方使用**私钥签名**、公开公钥，接收方使用**公钥验证**

私钥只有发送方拥有 -> 数字签名无法伪造

DNSSEC的工作位置

域名所有者（权威服务器）：**生成各资源记录（集）的数字签名**，塞进响应报文中

递归域名服务器：使用公钥**验证响应报文中的数字签名**



DNSSEC的工作原理：概述

数字签名（Digital signature）：发送方签名、接收方验证

发送方使用**私钥签名**、公开公钥，接收方使用**公钥验证**

私钥只有发送方拥有 –> 数字签名无法伪造

DNSSEC的工作位置

域名所有者（权威服务器）：**生成各资源记录（集）的数字签名**，塞进响应报文中

递归域名服务器：使用公钥**验证响应报文中的数字签名**

DNSSEC的核心工作流程

（一）域名所有者提供数字签名

（二）域名所有者构建信任链

（三）递归域名服务器验证响应

（一）域名所有者提供数字签名

域名所有者生成密钥对

ZSK：用于签名普通资源记录

KSK：用于签名公钥资源记录（DNSKEY）

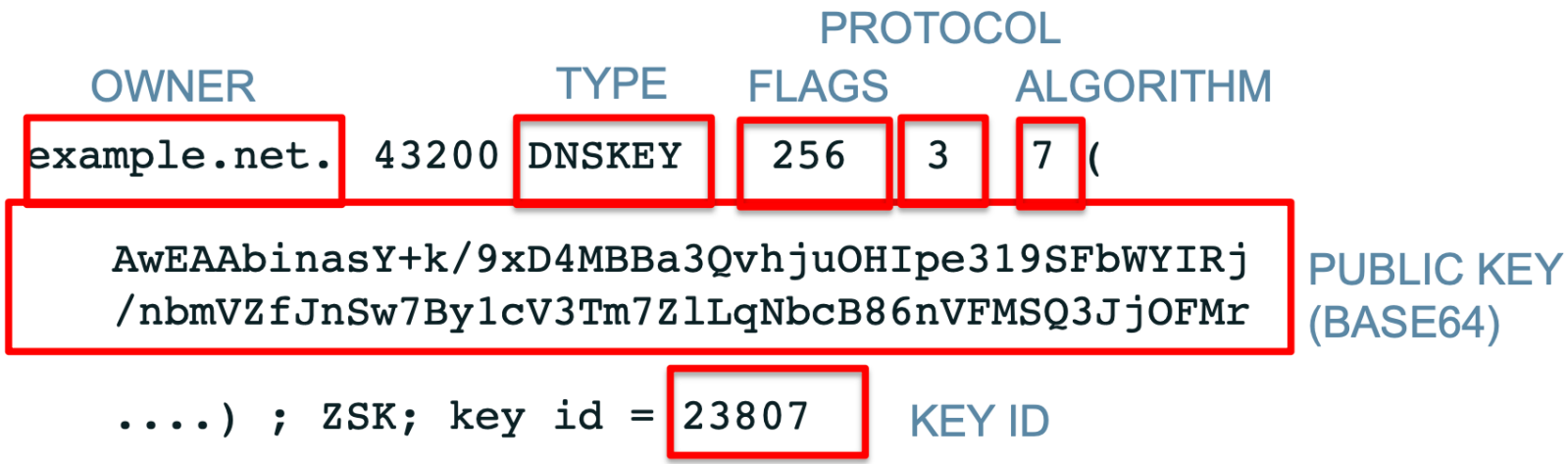
（一）域名所有者提供数字签名

域名所有者生成密钥对

ZSK：用于签名普通资源记录

KSK：用于签名公钥资源记录（DNSKEY）

创建**DNSKEY类型资源记录**：存储并对外公开公钥，便于递归服务器验证



（一）域名所有者提供数字签名

域名所有者生成密钥对

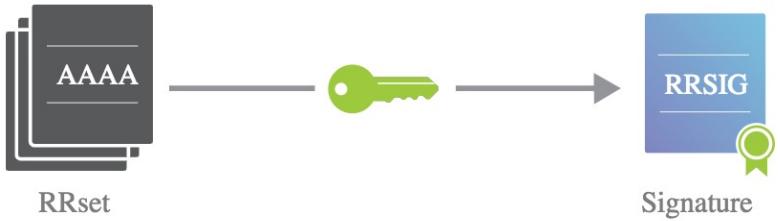
ZSK：用于签名普通资源记录

KSK：用于签名公钥资源记录（DNSKEY）

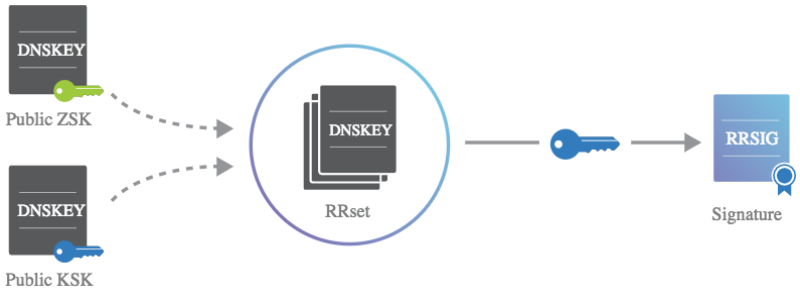
创建**DNSKEY类型资源记录**：存储并对外公开公钥，便于递归服务器验证

为每个资源记录集提供数字签名

RRSIG资源记录：存储数字签名，将被附带在权威服务器的响应报文中



使用ZSK对普通资源记录进行签名



使用KSK对公钥资源记录进行签名

（一）域名所有者提供数字签名

RRSIG资源记录

```
example.net.   600   A   192.168.10.10
example.net.   600   A   192.168.23.45
```

TYPE COVERED #LABELS

OWNER | TYPE | ALG | TTL

```
example.net.  600  RRSIG  A  7  2  600  (
```

SIG. EXPIRATION | SIG. INCEPTION | KEY ID | SIGNER NAME

```
20150115154303  20141017154303  23807  example.net.
```

SIGNATURE

```
CoYkYPqE8Jv6UaVJgRrh7u16m/cEFGtFM8TArbJdaiPu
W77wZhrvonoBEyqYbhQ1yDaS74u9whECEe08gfoe1FGg
. . .
)
```

（一）域名所有者提供数字签名

```
▼ Domain Name System (query)
    [Response In: 80]
    Transaction ID: 0x032c
  ▶ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▶ paypal.com: type A, class IN
  ▼ Additional records
    ▼ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▼ Z: 0x8000
          1... .... .... .... = DO bit: Accepts DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
```

请求报文

通过附加记录中的DO位

希望服务器返回DNSSEC相关记录

```
▼ Domain Name System (response)
    [Request In: 78]
    [Time: 0.091791000 seconds]
    Transaction ID: 0x032c
  ▶ Flags: 0x81a0 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▶ paypal.com: type A, class IN
  ▼ Answers
    ▼ paypal.com: type A, class IN, addr 64.4.250.36
        Name: paypal.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 72
        Data length: 4
        Address: 64.4.250.36
    ▶ paypal.com: type A, class IN, addr 64.4.250.37
    ▼ paypal.com: type RRSIG, class IN
        Name: paypal.com
        Type: RRSIG (46)
        Class: IN (0x0001)
        Time to live: 72
        Data length: 158
        Type Covered: A (Host Address) (1)
        Algorithm: RSA/SHA1 (5)
        Labels: 2
        Original TTL: 300 (5 minutes)
        Signature Expiration: Aug 14, 2022 20:05:36.000000000 CST
        Signature Inception: Jul 15, 2022 19:34:50.000000000 CST
        Key Tag: 11811
        Signer's name: paypal.com
        Signature: 6d00ab5e2bda2b1c63d27db831279897538385e2cc6fb9d4...
```

响应报文

在提供解析结果的同时，携带RRSIG签名记录

（一）域名所有者提供数字签名

密钥生成工具：dnssec-keygen

生成ZSK：`dnssec-keygen -a NSEC3RSASHA1 -b 2048 -n ZONE example.com`

生成KSK：`dnssec-keygen -f KSK -a NSEC3RSASHA1 -b 4096 -n ZONE example.com`

添加DNSKEY记录到区域文件：

```
for key in `ls Kexample.com*.key`
do
echo "\$INCLUDE $key">> example.com.zone
done
```

区域文件签名工具：dnssec-signzone

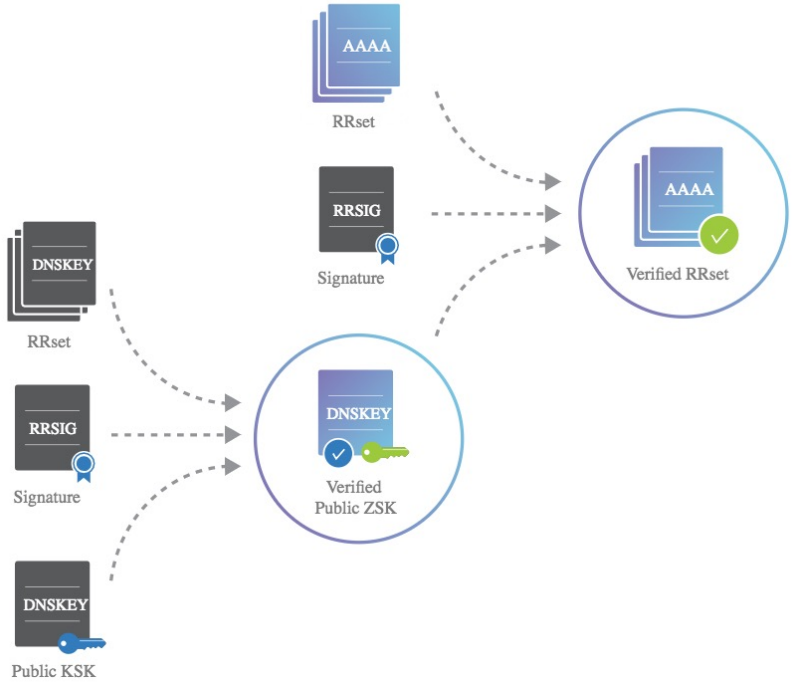
同时生成签名后的区域文件以及DS记录

```
dnssec-signzone -3 <salt> -A -N INCREMENT -o <zonename> -t <zonefilename>
```

配置方法参考：https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server-2

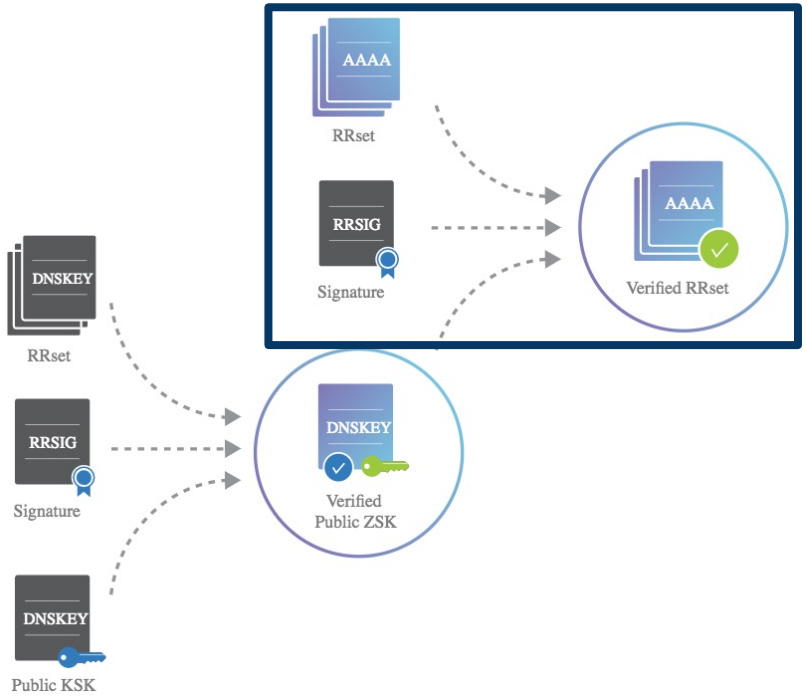
（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷



（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷

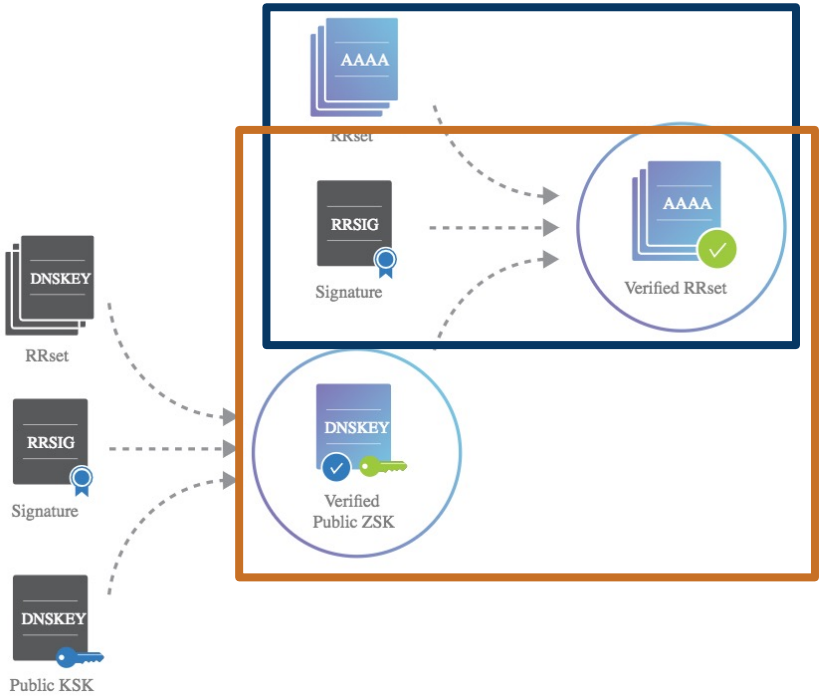


1．普通资源记录正确

必要条件：签名通过验证

（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷

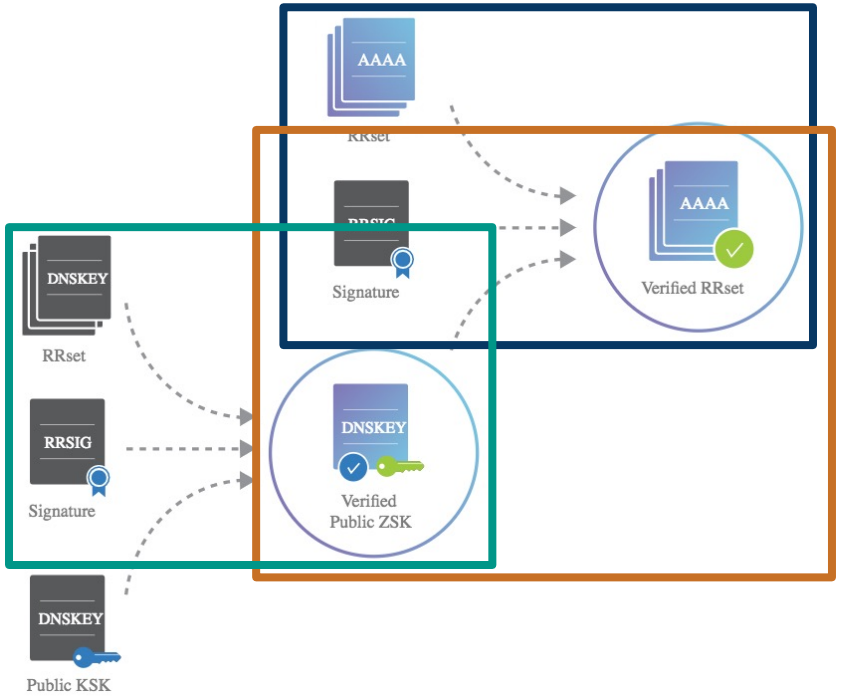


1． 普通资源记录正确
必要条件：签名通过验证

2． 签名通过验证
必要条件：公钥正确

（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷



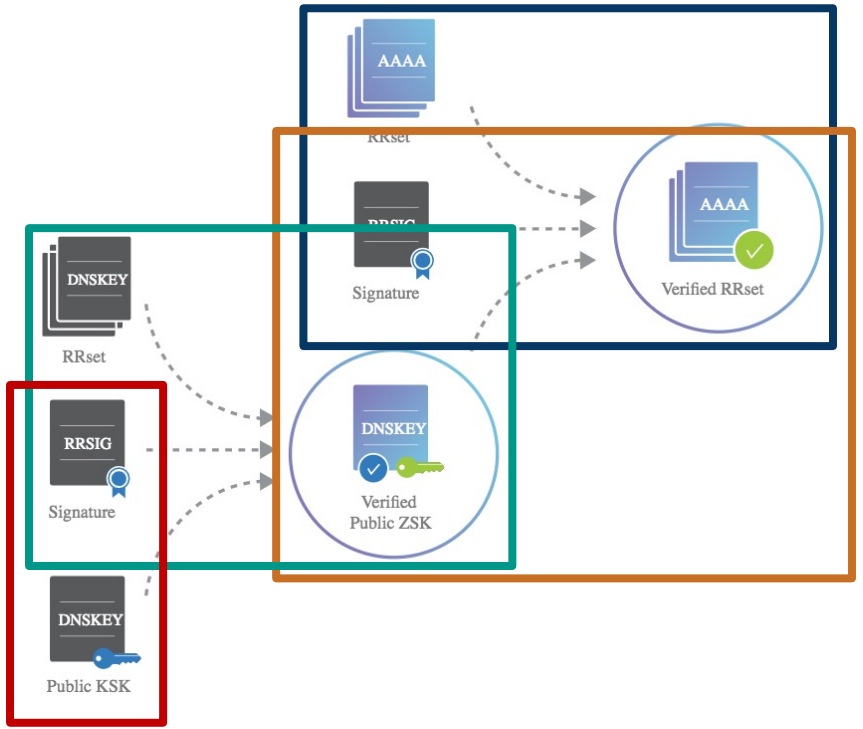
1．普通资源记录正确
必要条件：签名通过验证

2．签名通过验证
必要条件：公钥正确

3．公钥正确
必要条件：公钥自身的签名通过验证

（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷



1．普通资源记录正确
必要条件：签名通过验证

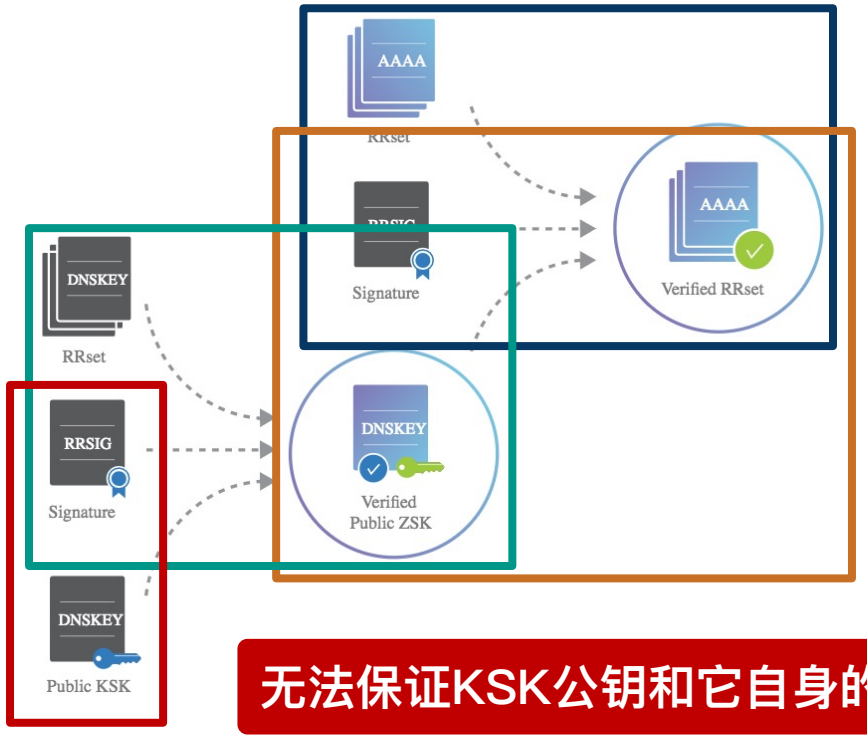
2．签名通过验证
必要条件：公钥正确

3．公钥正确
必要条件：公钥自身的签名通过验证

4．公钥自身的签名通过验证
必要条件：KSK公钥正确

（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷



1．普通资源记录正确
必要条件：签名通过验证

2．签名通过验证
必要条件：公钥正确

3．公钥正确
必要条件：公钥自身的签名通过验证

4．公钥自身的签名通过验证
必要条件：KSK公钥正确

无法保证KSK公钥和它自身的签名不被同时篡改

（二）域名所有者构建信任链

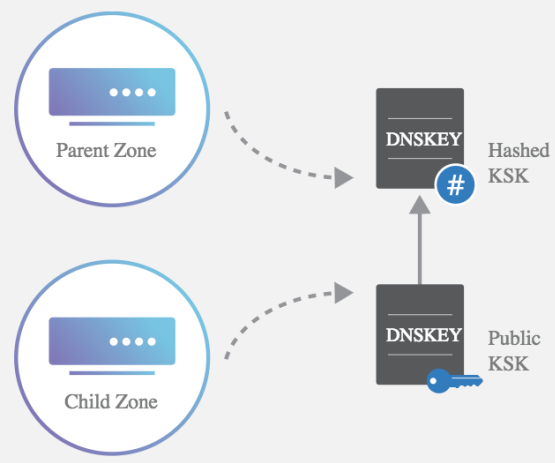
当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷

问题：信任关系停留在本级域名的KSK，攻击者可以同时篡改

解决方法：将信任链延伸至上级域名

如何保证KSK公钥正确、加大伪造难度：**上级域名存储KSK公钥的摘要（DS记录）**

一级一级向上延展，直到DNS根



（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷

问题：信任关系停留在本级域名的KSK，攻击者可以同时篡改

解决方法：将信任链延伸至上级域名

如何保证KSK公钥正确、加大伪造难度：**上级域名存储KSK公钥的摘要（DS记录）**

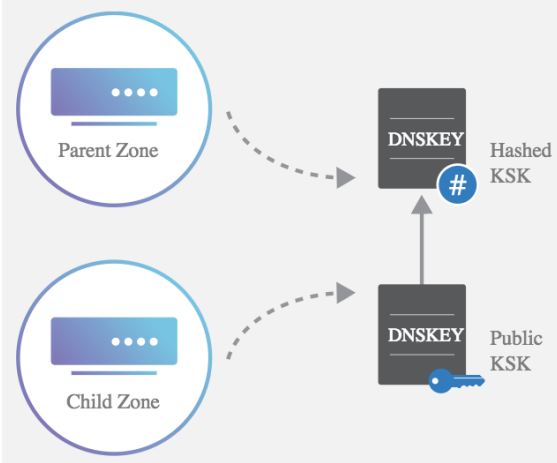
一级一级向上延展，直到DNS根

Digest type 1 = SHA-1, 2 = SHA-256

```
myzone.    DS  61138    5  1
F6CD025B3F5D0304089505354A0115584B56D683

myzone.    DS  61138    5  2
CCBC0B557510E4256E88C01B0B1336AC4ED6FE08C8268CC1AA5FBF00 5DCE3210
```

DS记录的基本格式



（二）域名所有者构建信任链

当域名所有者提供了数字签名和公钥，此时的信任关系仍有缺陷

问题：信任关系停留在本级域名的KSK，攻击者可以同时篡改

解决方法：将信任链延伸至上级域名

如何保证KSK公钥正确、加大伪造难度：**上级域名存储KSK公钥的摘要（DS记录）**

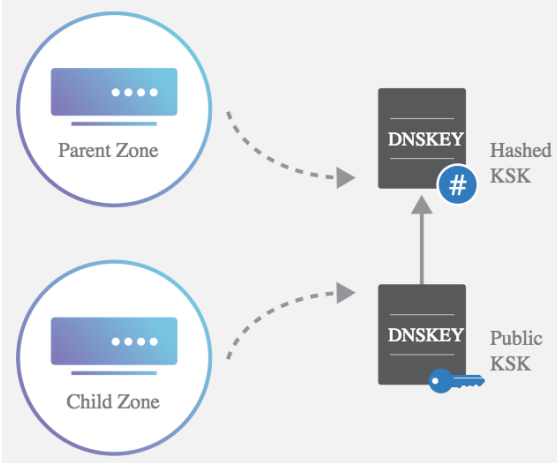
一级一级向上延展，直到DNS根

DNS根密钥

整个DNSSEC的信任锚点

由互联网社区多方监督审计产生，对根区签名

一般每5年轮换一次（下一次预计在2024年）



（二）域名所有者构建信任链

怎样上传DS记录到上级域名（通常意味着顶级域）？

一般域名，通过域名注册商提供的接口

阿里云（万网）提供的DS记录上传接口

教育网域名，需要上传至edu.cn
联系主管部门处理

（二）域名所有者构建信任链

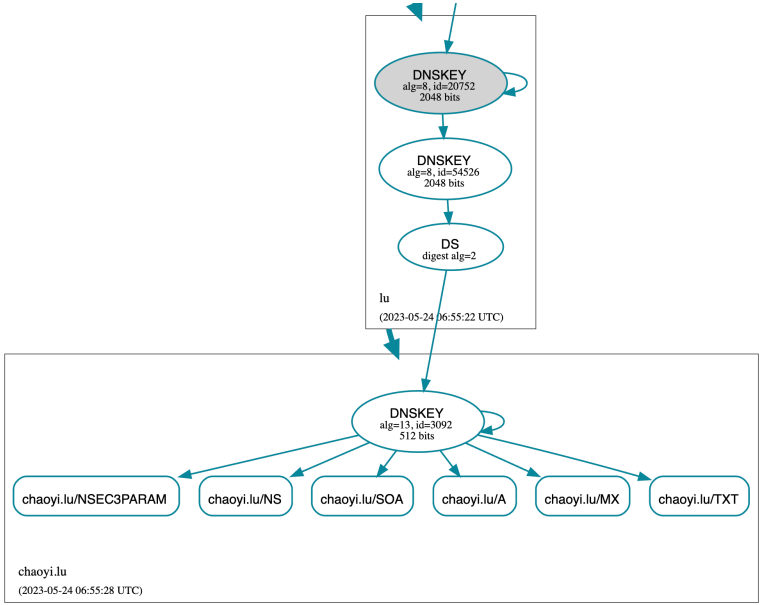
验证DNSSEC配置部署正确：在线工具

DNSViz：https://dnsviz.net/

Verisign DNSSEC Analyzer：https://dnssec-analyzer.verisignlabs.com/

Analyzing DNSSEC problems for chaoyi.lu

.	Found 2 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
lu	Found 1 DS records for lu in the . zone DS=20752/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=60955 and DNSKEY=60955 verifies the DS RRset Found 2 DNSKEY records for lu DS=20752/SHA-256 verifies DNSKEY=20752/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20752 and DNSKEY=20752/SEP verifies the DNSKEY RRset
chaoyi.lu	Found 1 DS records for chaoyi.lu in the lu zone DS=3092/SHA-256 has algorithm ECDSAP256SHA256 Found 1 RRSIGs over DS RRset RRSIG=54526 and DNSKEY=54526 verifies the DS RRset Found 1 DNSKEY records for chaoyi.lu DS=3092/SHA-256 verifies DNSKEY=3092 Found 1 RRSIGs over DNSKEY RRset RRSIG=3092 and DNSKEY=3092 verifies the DNSKEY RRset ns-89-a.gandi.net is authoritative for chaoyi.lu chaoyi.lu A RR has value 185.199.111.153 Found 1 RRSIGs over A RRset RRSIG=3092 and DNSKEY=3092 verifies the A RRset



（三）递归域名服务器验证响应

主动/被动获取DNSSEC相关的所有资源记录，并进行验证

主动查询：本级域名的公钥

被动获取：上级域名给的摘要、本级域名给的签名

3． 验证资源记录

使用经过验证的ZSK公钥

2． 验证ZSK公钥

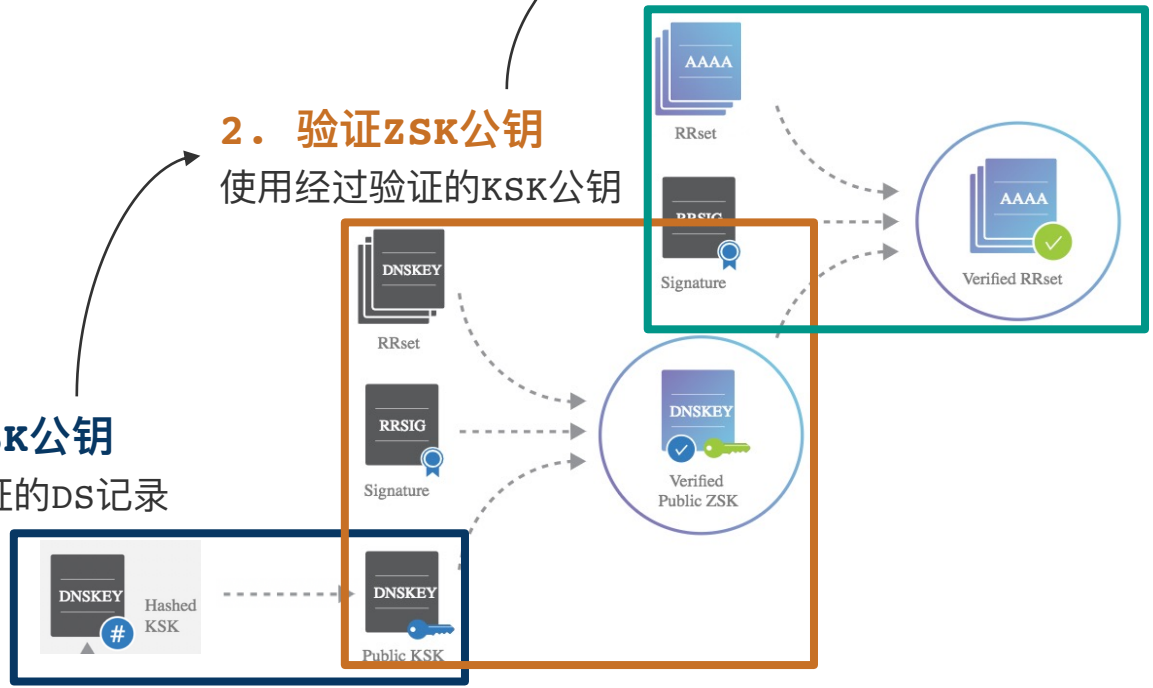
使用经过验证的KSK公钥

1． 验证KSK公钥

使用经过验证的DS记录

0． 验证从上级域名获得的DS记录

使用上级域名的签名和密钥



总结

DNSSEC的部署应用，由域名所有者和递归域名服务器共同完成

角色	要做的事	具体步骤和技术方案
域名所有者	提供数字签名	1. 生成密钥对（ZSK、KSK）
		2. 生成DNSKEY资源记录，公开公钥
		3. 对每个资源记录集进行正确签名，生成RRSIG资源记录
		4. 对数字签名和密钥对进行定时更新
	构建信任链	5. 计算KSK摘要，生成DS资源记录
		6. 上传DS资源记录至上级域名
递归服务器	验证响应报文	使用主流DNS软件，配置开启并测试DNSSEC验证功能

第三部分　Part III

DNSSEC的部署应用现状

DNSSEC的部署应用——远不及预期

DNSSEC自身经历了多个版本迭代

90年代，已废止的方案：RFC2065 (1997)、RFC2535 (1999)

现行标准方案：**RFC4033、RFC4034、RFC4035 (2005)**

根区文件签名：2010年完成

DNSSEC的部署应用——远不及预期

DNSSEC自身经历了多个版本迭代

90年代，已废止的方案：RFC2065 (1997)、RFC2535 (1999)

现行标准方案：**RFC4033、RFC4034、RFC4035 (2005)**

根区文件签名：2010年完成

十余年后：部署应用情况

部署率低：主流顶级域（.com/.net/.org）下的二级域名，**签名率不足5%**

验证率低：超过80%的递归域名服务器未进行签名验证 [Chung 17]

时间	域名签名率	部分顶级域下的二级域名签名率							
		.com	.net	.org	.bank	.cz	.nl	.no	.sk
2017 年 1 月	1.0%	0.7%	1.0%	1.1%	-	-	-	-	-
2022 年 1 月	3.4%	2.7%	3.1%	2.9%	60.7%	51.0%	43.8%	40.8%	37.7%

DNSSEC的部署应用——远不及预期

DNSSEC自身经历了多个版本迭代

90年代，已废止的方案：RFC2065 (1997)、RFC2535 (1999)

现行标准方案：**RFC4033、RFC4034、RFC4035 (2005)**

根区文件签名：2010年完成

十余年后：部署应用情况

部署率低：主流顶级域（.com/.net/.org）下的二级域名，**签名率不足5%**

验证率低：超过80%的递归域名服务器未进行签名验证 [Chung 17]

时间	域名签名率	部分顶级域下的二级域名签名率							
		.com	.net	.org	.bank	.cz	.nl	.no	.sk
2017 年 1 月	1.0%	0.7%	1.0%	1.1%	-	-	-	-	-
2022 年 1 月	3.4%	2.7%	3.1%	2.9%	60.7%	51.0%	43.8%	40.8%	37.7%

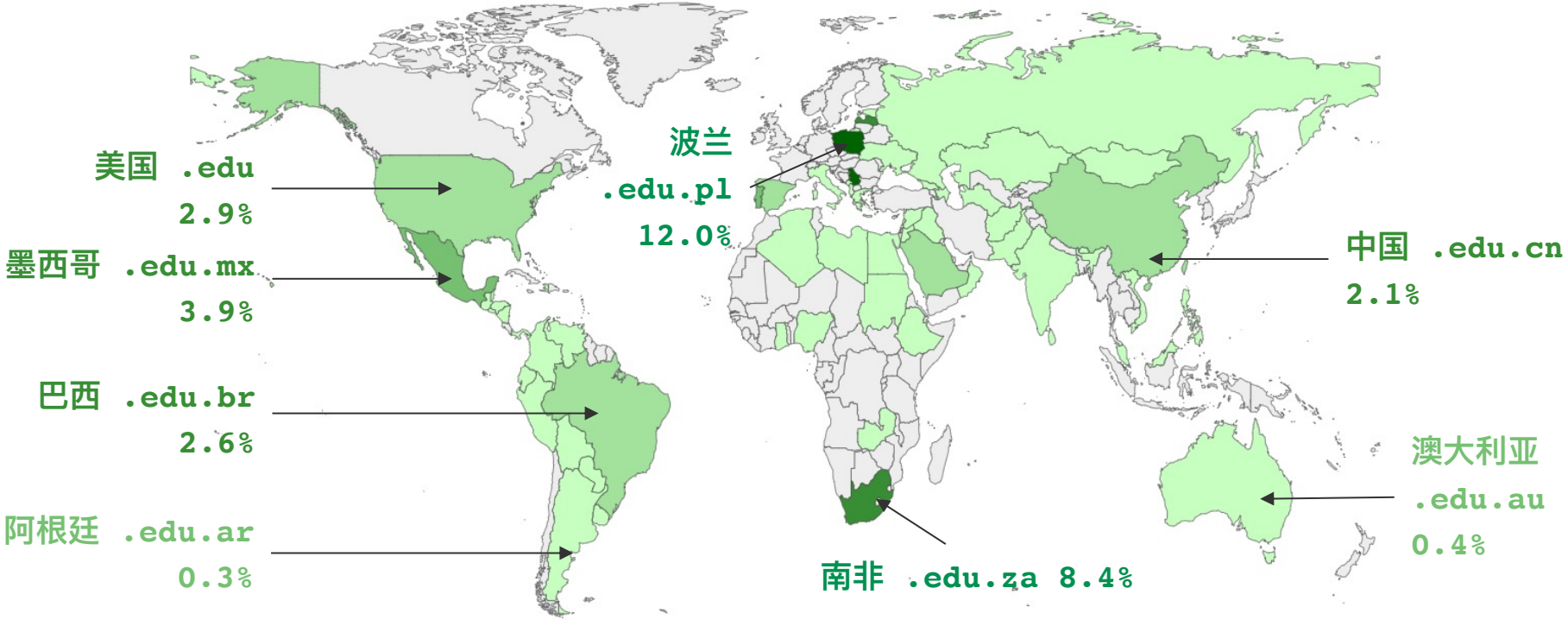
特定行业/顶级域

DNSSEC的部署应用情况较好

重点行业域名的DNSSEC部署应用情况

教育域名的DNSSEC签名情况：全球

截至2023年5月，教育行业域名的正确签名情况**仍不理想**，仅个别国家超过5%



重点行业域名的DNSSEC部署应用情况

教育域名的DNSSEC签名情况：国内

截至2023年5月，总体域名签名率38/1843=2.1%

www.hfut.edu.cn	www.hfuu.edu.cn	www.fjut.edu.cn	www.fjnu.edu.cn	www.lnut.edu.cn
www.ahpu.edu.cn	www.whit.edu.cn	www.zjc.edu.cn	www.szu.edu.cn	www.ujn.edu.cn
www.bbmc.edu.cn	www.xcvtc.edu.cn	www.neu.edu.cn	www.gxnu.edu.cn	www.shec.edu.cn
www.fynu.edu.cn	www.afc.edu.cn	www.nwafu.edu.cn	www.guat.edu.cn	www.tfswufe.edu.cn
www.aqnu.edu.cn	www.hfnu.edu.cn	www.sjtu.edu.cn	www.gzu.edu.cn	www.nankai.edu.cn
www.chzu.edu.cn	www.hfpec.edu.cn	www.ustc.edu.cn	www.htu.edu.cn	www.tju.edu.cn
www.aufe.edu.cn	www.ahou.edu.cn	www.ahau.edu.cn	www.csust.edu.cn	
www.tlu.edu.cn	acsxy.aufe.edu.cn	www.bupt.edu.cn	www.hnfnu.edu.cn	

重点行业域名的DNSSEC部署应用情况

教育域名的DNSSEC签名情况：国内

截至2023年5月，总体域名签名率38/1843=2.1%

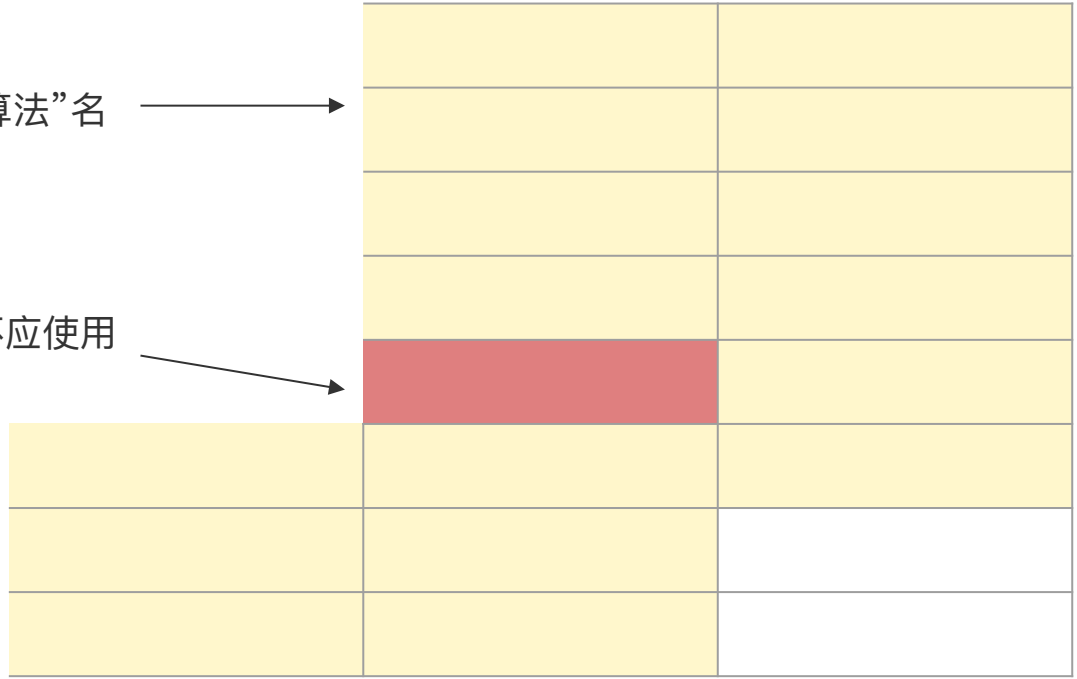
偏弱的密钥算法(16/38)：

使用的算法被RFC8624列入“不推荐算法”名单

亟需更换的密钥算法(1/38)：

使用DSA算法，已被RFC8624列入“不应使用算法”名单

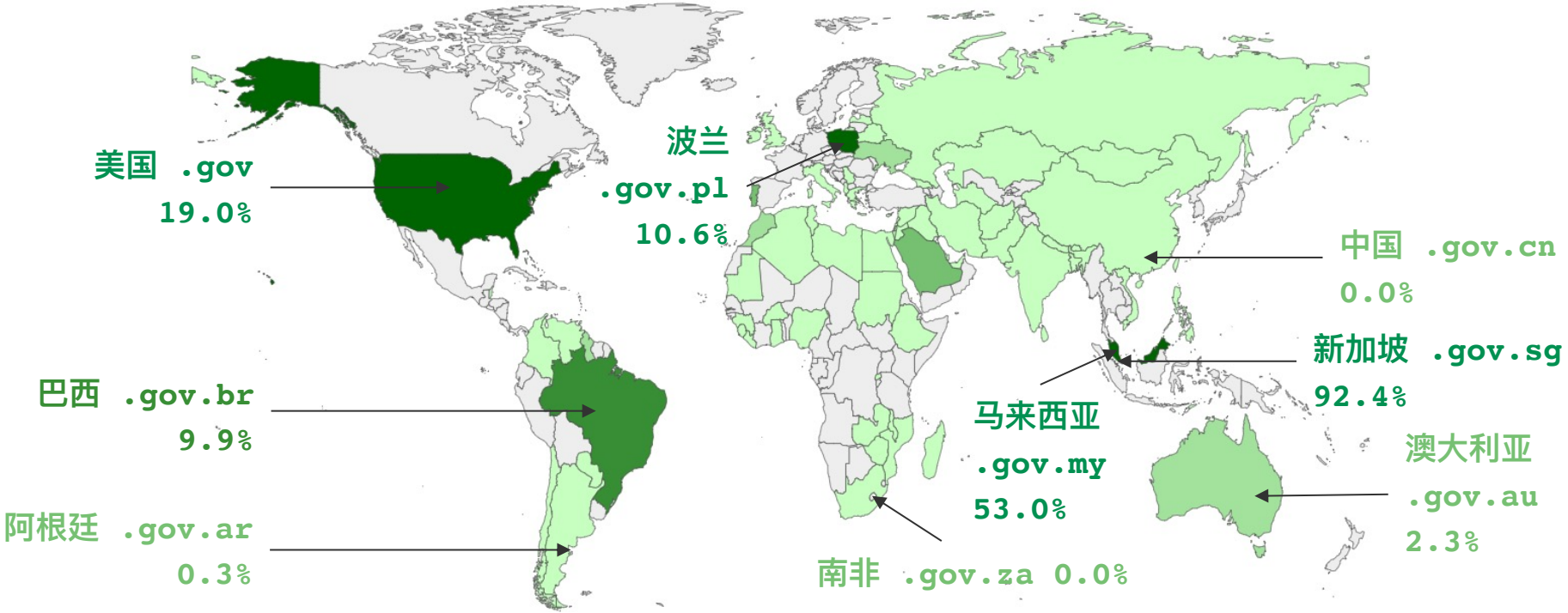
此外，该域名签名已超过有效期



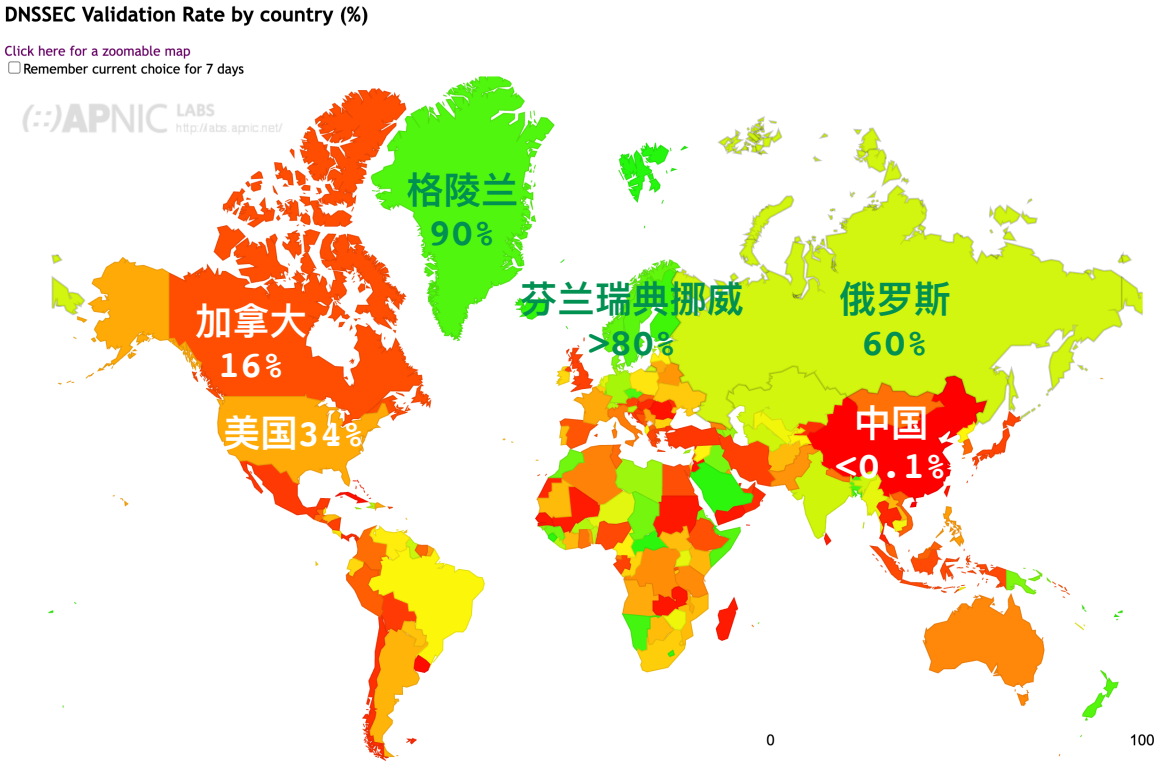
重点行业域名的DNSSEC部署应用情况

政府域名的DNSSEC签名情况：全球

截至2023年5月，政府行业域名的正确签名情况**在部分国家更为充分**



服务器对DNSSEC签名的验证情况



在多数国家，

服务器对DNSSEC签名的验证

比例仍然较低

推动DNSSEC的部署
需要域名所有者、域名
服务器的共同参与

https://stats.labs.apnic.net/dnssec

第四部分　Part IV

DNSSEC的配置注意事项

哪些步骤容易出问题?

角色	要做的事	具体步骤和技术方案
域名所有者	提供数字签名	1. 生成密钥对（ZSK、KSK）
		2. 生成DNSKEY资源记录，公开公钥
		3. 对每个资源记录集进行正确签名，生成RRSIG资源记录
		4. 对数字签名和密钥对进行定时更新
	构建信任链	5. 计算KSK摘要，生成DS资源记录
		6. 上传DS资源记录至上级域名
递归服务器	验证响应报文	使用主流DNS软件，配置开启并测试DNSSEC验证功能

哪些步骤容易出问题?

注意密钥算法的强度

使用推荐算法，及时淘汰过时/不推荐的算法

算法推荐列表：RFC 8624

Number	Mnemonics	DNSSEC Signing	DNSSEC Validation
1	RSAMD5	MUST NOT	MUST NOT
3	DSA	MUST NOT	MUST NOT
5	RSASHA1	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST
8	RSASHA256	MUST	MUST
10	RSASHA512	NOT RECOMMENDED	MUST
12	ECC-GOST	MUST NOT	MAY
13	ECDSAP256SHA256	MUST	MUST
14	ECDSAP384SHA384	MAY	RECOMMENDED
15	ED25519	RECOMMENDED	RECOMMENDED
16	ED448	MAY	RECOMMENDED

RFC 8624：https://www.rfc-editor.org/rfc/rfc8624.html

哪些步骤容易出问题?

注意数字签名的有效期

通常情况下，DNSSEC签名有效期为若干天/月量级

在过期前及时更新，**避免因超过有效期而无法通过验证**

```
;; ANSWER SECTION:
chaoyi.lu.              3600    IN      A       185.199.110.153
chaoyi.lu.              3600    IN      A       185.199.111.153
chaoyi.lu.              3600    IN      A       185.199.108.153
chaoyi.lu.              3600    IN      A       185.199.109.153
chaoyi.lu.              3600    IN      RRSIG   A 13 2 3600 20230601000000 20230511000000 3092 chaoyi.lu. 6uP6YM1Tae8HS4rfU6eZaSHNwE9sazd8iEkcgwk9519HcYB9ECwZ9py8 PAsWsExUhrAvGED3GgXbsXRSkOHwbg==
```

本数字签名有效期为20天

哪些步骤容易出问题?

注意数字签名的有效期

通常情况下，DNSSEC签名有效期为若干天/月量级

在过期前及时更新，**避免因超过有效期而无法通过验证**

```
;; ANSWER SECTION:
chaoyi.lu.              3600    IN      A       185.199.110.153
chaoyi.lu.              3600    IN      A       185.199.111.153
chaoyi.lu.              3600    IN      A       185.199.108.153
chaoyi.lu.              3600    IN      A       185.199.109.153
chaoyi.lu.              3600    IN      RRSIG   A 13 2 3600 20230601000000 20230511000000 3092 chaoyi.lu. 6uP6YM1Tae8HS4rfU6eZaSHNwE9sazd8iEkcgwk9519HcYB9ECwZ9py8 PAsWsExUhrAvGED3GgXbsXRSkOHwbg==
```

本数字签名有效期为20天

务必上传公钥摘要（DS）至上级域名

可能需要**联系顶级域注册局/注册商**处理

无DS记录的域名，会被递归域名服务器视作未部署DNSSEC，无法受到安全保障

哪些步骤容易出问题?

附：教育网edu.cn域名技术检查项（1）

地址检查	
是否有反向解析记录	用于域名服务器的 IPv4、IPv6 地址需有反向解析记录
是否支持 IPv4	至少有 1 个 IPv4 服务地址
是否支持 IPv6	至少有 1 个 IPv6 服务地址
连通性	
UDP 53 端口服务的可用性	
TCP 53 端口服务的可用性	
DNSSEC 相关检查	
使用 NSEC3	必须使用 NSEC3，以防止对区数据的遍历
DS 记录格式	需要提供 DS 记录的 4 个属性值，key tag、key 算法、摘要类型、摘要内容；各属性值均符合要求；
是否有匹配的 DNSKEY 记录	提出申请时，域名服务器应该配置与提交的 DS 匹配的 DNSKEY 记录。
验证 RRSIG 记录	查询 SOA 记录，根据提交的 DS 记录，对 RRSIG 记录进行验证（查询结果需有 DO 位）

哪些步骤容易出问题?

附：教育网edu.cn域名技术检查项（2）

域名服务器	
域名服务器数量	不低于 2 个，且指向不同地址
域名服务器名称有效	参考 RFC1123, 2.1 节
给出权威应答	域名服务器必须提供所注册域名的权威服务
授权记录和权威数据的一致性	在父区（edu.cn）的授权记录与本区配置的权威记录一致
权威服务器的数据一致性	所有域名服务器的 NS 记录一致，SOA 记录一致
NS 记录的应答不超过 512 字节	应答包括 NS 记录及必要的 glue 记录
是否开启递归	必须关闭递归服务
是否支持 edns0	必须支持
是否允许发起全量区传送	建议关闭