ICS 33.040.40
CCS L79

YD

中华人民共和国通信行业标准

YD/T XXX—XXXX

域名系统解析数据加密传输技术要求

Domain name system resolution data encryption transmission technical requirements

（报批稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国工业和信息化部　　发布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：清华大学、互联网域名系统北京市工程研究中心有限公司、赛尔网络有限公司、恒安嘉新（北京）科技股份公司、中兴通讯股份有限公司、中国信息通信研究院、中国科学院信息工程研究所、四川天邑康和通信股份有限公司。

本文件部分主要起草人：陆超逸、黄友俊、张甲、段海新、马迪、张云飞、刘知刚、邓斌、李威、孙科、林兆骥、谢家贵、谭建龙、刘燕兵、何芯锐。

域名系统解析数据加密传输技术要求

1 范围

本文件规定了域名系统解析数据加密传输技术的协议设计规范和部署要求。

本文件适用于域名系统中的解析数据传输，包括用户到递归DNS服务器之间的数据传输，以及用户直接访问权威DNS服务器之间的数据传输。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 1035 域名 实施和规范（DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION）

IETF RFC 7830 基于DNS扩展的填充机制（The EDNS(0) Padding Option）

IETF RFC 8467 使用DNS扩展机制的填充策略(Padding Policies for Extension Mechanisms for DNS (EDNS(0))）

3 术语和定义

下列术语和定义适用于本文件。

3.1

递归域名服务器 recursive DNS resolver（rDNS）

递归执行域名解析任务，并返回解析结果的服务器。

3.2

权威域名服务器 authoritative DNS server（aDNS）

存储特定域名解析数据，并负责提供该域解析服务的服务器。

4 缩略语

下列缩略语适用于本文件。

CA	证书颁发机构	Certificate Authority
DNS	域名服务	Domain Name System
DoD	基于数据报传输层安全协议的域名服务	DNS over DTLS
DoH	基于超文本传输安全协议的域名服务	DNS Queries over HTTPS
DoQ	基于快速用户数据报协议的域名服务	DNS over QUIC
DoT	基于传输层安全协议的域名服务	DNS over TLS
DTLS	数据报传输层安全协议	Datagram Transport Layer Security
EDNS0	域名服务扩展机制	Extension Mechanisms for DNS
QUIC	快速用户数据报网络连接协议	Quick UDP Internet Connection

TCP	传输控制协议	Transmission Control Protocol
TLS	传输层安全协议	Transport Layer Security
UDP	用户数据报协议	User Datagram Protocol

5 域名系统解析数据加密传输的体系结构

5.1 域名系统的体系结构

域名系统（Domain Name System，DNS）提供互联网域名至数字地址的映射关系。域名系统的基本体系结构由DNS用户、递归DNS服务器和权威DNS服务器组成。DNS用户可通过查询递归DNS服务器，也可通过直接查询权威DNS服务器获得域名解析结果。递归DNS服务器可通过查询权威DNS服务器获得域名解析结果，也可通过转发至上一级递归DNS服务器进行查询。如图1所示，在一次完整的域名解析过程中，DNS用户向递归DNS服务器发起域名查询请求（图1，第1步），递归DNS服务器应依次查询根服务器（图1，第2步）、顶级域权威服务器（图1，第3步）、二级域权威服务器等权威DNS服务器（图1，第4步），并返回查询结果至DNS用户（图1，第5步）。

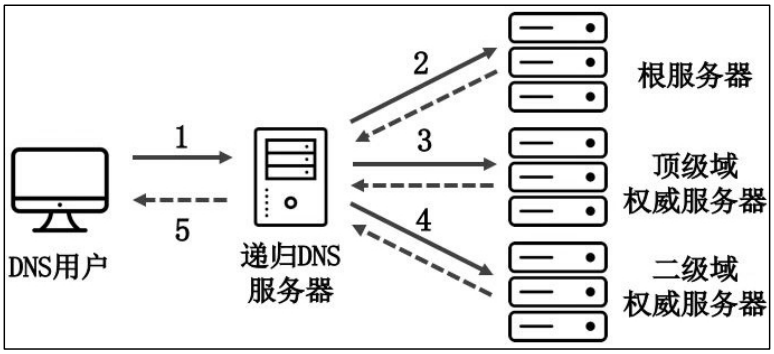

图1 域名系统体系结构

5.2 域名系统解析数据加密传输工作位置

5.2.1 用户至递归 DNS 服务器

使用域名系统解析数据加密传输协议，保护DNS用户至递归DNS服务器之间的查询不被窃听或劫持。适用于DNS用户依赖递归DNS服务器的情况。其工作位置如图2所示。国际上目前的标准方案DNS-over-TLS（参见IETF RFC 7858）和DNS-over-HTTPS（参见 IETF RFC 8484）均工作于此位置。

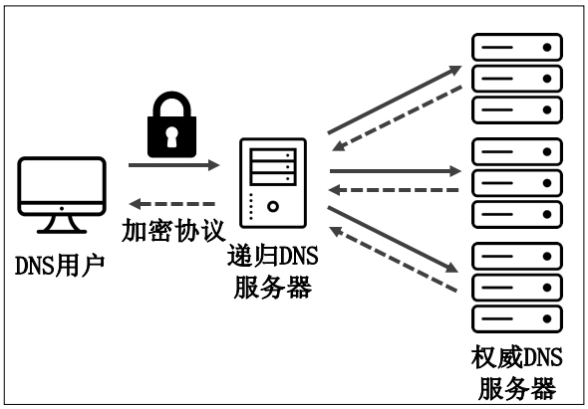

图2 用户至递归 DNS 服务器的域名解析数据加密传输

5.2.2 用户至权威 DNS 服务器

如图3所示，使用域名系统解析数据加密传输协议，保护DNS用户至权威DNS服务器之间的查询不被窃听或劫持，适用于DNS用户直接查询权威DNS服务器的情况。此时，用户的DNS查询应不依赖递归DNS服务器，而直接向权威DNS服务器发起加密DNS通信。

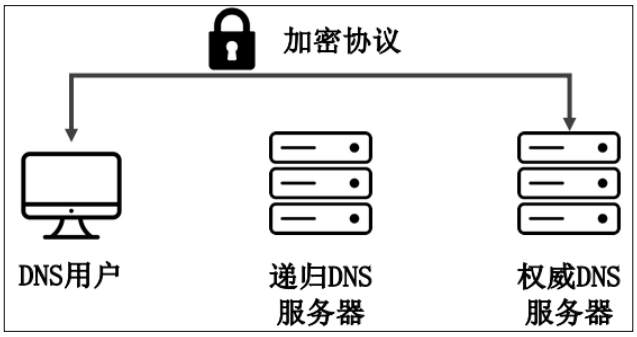

图3 用户至权威 DNS 服务器的域名解析数据加密传输

5.2.3 用户至 DNS 服务器通信接口

使用DoT时，DNS服务器应申请域名证书以进行身份验证，应配置DNS服务器的端口、申请域名证书后的证书和密钥路径。用户应在支持DoT的终端系统中指定DNS服务器。

使用DoH时，DNS服务器应申请域名证书以进行身份验证。用户应在支持DoH的终端浏览器或其他应用中指定DNS服务器。

使用DoQ时，DNS服务器应申请域名证书以进行身份验证，应配置DNS服务器的端口、申请域名证书后的证书和密钥路径。用户应在支持DoQ的终端系统中指定DNS服务器。

使用DoD时，DNS服务器应申请域名证书以进行身份验证，应配置DNS服务器的端口、申请域名证书后的证书和密钥路径。用户应在支持DoD的终端系统中指定DNS服务器。

用户查询递归DNS服务器时，递归DNS服务器应支持用户所使用协议。

用户查询权威DNS服务器时，权威DNS服务器应支持用户所使用协议。

6 数据交换接口和传输机制

6.1 传输层协议

域名系统解析数据加密通信在传输层使用TCP或UDP协议。例如，基于TLS的域名系统加密通信使用TCP（例如DoT和DoH）；基于QUIC或DTLS的域名系统加密通信使用UDP（例如DoQ和DoD）。

传输层使用TCP协议时，DNS客户端在发起加密请求之前与DNS服务器通过三次握手建立TCP连接。此时，域名系统解析数据加密通信应执行基于TCP的DNS传输最佳实践（参见IETF RFC 7766，6.2节）：

a) 支持连接复用和状态保持；

b) 支持并行请求处理；

c) 支持连接超时处理；

d) 支持连接关闭。

6.2 加密信道建立和身份认证

6.2.1 加密参数协商

域名系统解析数据加密传输的通信双方在发起加密DNS请求之前，使用加密通信协议建立加密信道并协商参数。协商的内容主要包括：加密协议版本、加密算法、密钥等。

在选取加密算法时，根据通信双方的支持情况，应符合相关的密码国家标准。

6.2.2 基于证书的身份认证

DNS客户端在DNS查询前应对服务器的身份进行验证。参照IETF RFC 8310中第8节的规定，DNS客户端使用基于认证域名（ADN）或证书主体公钥（SPKI）的方式对服务器提供的TLS证书进行认证；客户端对服务器提供的完整证书链进行验证，检查证书是否由合法机构签发，并将证书中的主体名称与服务器名称进行匹配。

当身份认证不通过时，DNS客户端应将DNS服务器视为不可信。

6.3 连接复用和状态保持

当使用基于TCP或TLS的加密通信协议时，域名系统解析数据加密传输的通信双方在资源允许的情况下应保持加密信道，支持连接复用。通信双方在连接长时间空闲时应断开连接。根据目前的最佳实践，超时值的设置应以秒为单位（参见IETF RFC 7766，6.2.3节）。

当使用基于UDP的加密通信协议时，不必考虑连接复用。

6.4 并行请求处理

域名系统解析数据加密传输的通信双方，应支持同一连接中多个请求的并行处理。DNS客户端在发起一个域名查询后无需等待结果，可使用当前连接发送新的查询至DNS服务器。

6.5 错误处理

域名系统解析数据加密传输的通信双方，在加密信道出现错误时，可自主选择是否使用明文重新传输DNS数据。

7 协议数据单元

7.1 请求报文格式

域名系统解析数据加密传输中使用的DNS请求报文格式，应为DNS原始数据包格式。根据IETF RFC 1035中4.1节的规定，请求报文应含有DNS头部（包含DNS查询ID、DNS状态码、DNS标识位）和DNS数据（包含问题区域、回答区域、权威区域、补充区域及具体的DNS资源记录）。

7.2 响应报文格式

域名系统解析数据加密传输中使用的DNS响应报文格式，应为DNS原始数据包格式。根据IETF RFC 1035中4.1节的规定，响应报文应含有DNS头部（包含DNS查询ID、DNS状态码、DNS标识位）和DNS数据（包含问题区域、回答区域、权威区域、补充区域及具体的DNS资源记录）。

8 协议部署要求

8.1 加密协议版本

域名系统解析数据加密传输的通信双方，应使用TLS 1.2及以上版本。

8.2 加密算法和密钥

域名系统解析数据加密传输的通信双方，应使用强加密算法和密钥，信息系统中使用的密码算法应符合国家密码管理相关规定。

8.3 证书

域名系统解析数据加密传输的服务器端，应安装由可信根CA签发的有效TLS证书，并进行有效管理。

8.4 消息填充

域名系统解析数据加密传输的通信双方，应使用IETF RFC 7830和IETF RFC 8467定义的填充措施，使用EDNS(0)属性和附加的OPT DNS资源记录对请求和响应数据包进行填充。

参 考 文 献

【1】. GB/T 33134-2016 信息安全技术 公共域名服务系统安全要求
【2】. GB/T 33562-2017 信息安全技术 安全域名系统实施指南
【3】. YD/T 2137-2010 域名系统递归服务器运行技术要求
【4】. YD/T 2138-2010 域名系统权威服务器运行技术要求
【5】. YD/T 2140-2010 域名服务系统安全框架技术要求
【6】. YD/T 2052-2015 域名系统安全防护要求
【7】. YD/T 2053-2016 域名系统安全防护检测要求
【8】. DNS over Dedicated QUIC Connections（IETF draft）