Co se děje v DNS protokolu?

Ondřej Surý, ISC

CSNOG 2019

Photo by Hari Nandakumar on Unsplash

“…poslední stéblo, které zlomilo velbloudovi hřbet”

–orientální přísloví

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
882		Obsolete	Domain Names – Concepts and Facilities	x		x	x				x				
883		Obsolete	Domain Names – Implementation and Specification		x		x	x			x	x			
920			Domain Requirements				x								
973		Obsolete	Domain System Changes and Observations			x		x			x	x			
1032			Domain Administrators Guide				x								
1033			Domain Administrators Operations Guide				x								
1034	Standard		Domain Names – Concepts and Facilities	x		x	x			x	x	x			
1035	Standard		Domain Names – Implementation and Specification		x	x		x			x	x	x		
1101			DNS Encoding of Network Names and Other Types			x									
1123	Standard		Requirements for Internet Hosts – Application and Support	x							x	x			
1178	Informational		Choosing a Name for Your Computer				x								
1183	Experimental		New DNS RR Definitions					x							
1348	Experimental	Obsolete	DNS NSAP RRs					x							
1401	Informational		Correspondence between the IAB and DISA on the use of DNS throughout the Internet	x											
1535	Informational		A Security Problem and Proposed Correction With Widely Deployed DNS Software									x			
1536	Informational		Common DNS Implementation Errors and Suggested Fixes							x		x			
1537	Informational	Obsolete	Common DNS Data File Configuration Errors				x								
1591	Informational		Domain Name System Structure and Delegation				x								
1611	Historic	Historic	DNS Server MIB Extensions				x								
1612	Historic	Historic	DNS Resolver MIB Extensions				x								

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
1637	Experimental	Obsolete	DNS NSAP Resource Records					x							
1664	Experimental	Obsolete	Using the Internet DNS to Distribute RFC1327 Mail Address Mapping Tables					x							
1706	Informational		DNS NSAP Resource Records					x							
1712	Experimental		DNS Encoding of Geographical Location					x							
1713	Informational		Tools for DNS Debugging				x								
1794	Informational		DNS Support for Load Balancing	x											
1876	Experimental		A Means for Expressing Location Information in the Domain Name System					x							
1886	Proposed	Obsolete	DNS Extensions to support IP version 6				x	x							
1912	Informational		Common DNS Data File Configuration Errors				x								
1982	Proposed		Serial Number Arithmetic		x		x								
1995	Proposed		Incremental Zone Transfer in DNS		x						x		x		
1996	Proposed		A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)		x						x		x		
2010	Informational	Obsolete	Operational Criteria for Root Name Servers				x								
2052	Experimental	Obsolete	A DNS RR for specifying the location of services (DNS SRV)					x							
2065	Proposed	Obsolete	Domain Name System Security Extensions	x			x	x			x	x			x
2100	Informational	April 1st	The Naming of Hosts												
2136	Proposed		Dynamic Updates in the Domain Name System (DNS UPDATE)		x						x			x	
2137	Proposed	Obsolete	Secure Domain Name System Dynamic Update		x						x			x	
2163	Proposed		Using the Internet DNS to Distribute MIXER Conformant Global Address Mapping (MCGAM)					x							
2168	Experimental	Obsolete	Resolution of Uniform Resource Identifiers using the Domain Name System					x							

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
2181	Proposed		Clarifications to the DNS Specification		x	x					x	x			
2182	BCP		Selection and Operation of Secondary DNS Servers				x								
2230	Informational		Key Exchange Delegation Record for the DNS					x							
2308	Proposed		Negative Caching of DNS Queries (DNS NCACHE)									x			
2317	BCP		Classless IN-ADDR.ARPA delegation				x								
2535	Proposed	Obsolete	Domain Name System Security Extensions					x			x	x	x		x
2536	Proposed		DSA KEYs and SIGs in the Domain Name System (DNS)					x							
2537	Proposed	Obsolete	RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)					x							
2538	Proposed	Obsolete	Storing Certificates in the Domain Name System (DNS)					x							
2539	Proposed		Storage of Diffie-Hellman Keys in the Domain Name System (DNS)					x							
2540	Experimental		Detached Domain Name System (DNS) Information		x										
2541	Informational	Obsolete	DNS Security Operational Considerations				x								
2606	BCP		Reserved Top Level DNS Names				x								
2671	Proposed	Obsolete	Extension Mechanisms for DNS (EDNS0)		x			x			x	x			
2672	Proposed	Obsolete	Non-Terminal DNS Name Redirection					x			x	x			
2673	Historic	Obsolete	Binary Labels in the Domain Name System		x						x	x			
2782	Proposed		A DNS RR for specifying the location of services (DNS SRV)					x							
2825	Informational		A Tangled Web: Issues of I18N, Domain Names, and the Other Internet protocols	x											
2826	Informational		IAB Technical Comment on the Unique DNS Root	x											
2845	Proposed		Secret Key Transaction Authentication for DNS (TSIG)		x			x			x	x			

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
2870	BCP		Root Name Server Operational Requirements				x								
2874	Historic	Historic	DNS Extensions to Support IPv6 Address Aggregation and Renumbering				x	x				x			
2915	Proposed	Obsolete	The Naming Authority Pointer (NAPTR) DNS Resource Record					x							
2929	BCP	Obsolete	Domain Name System (DNS) IANA Considerations	x							x	x			
2930	Proposed		Secret Key Establishment for DNS (TKEY RR)		x			x			x	x			
2931	Proposed		DNS Request and Transaction Signatures (SIG(0)s)					x			x	x			
3007	Proposed		Secure Domain Name System (DNS) Dynamic Update		x						x			x	x
3008	Proposed	Obsolete	Domain Name System Security (DNSSEC) Signing Authority												x
3071	Informational		Reflections on the DNS, RFC 1591, and Categories of Domains	x											
3090	Proposed	Obsolete	DNS Security Extension Clarification on Zone Status	x											x
3110	Proposed		RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)					x							
3123	Experimental		A DNS RR Type for Lists of Address Prefixes (APL RR)					x							
3130	Informational		Notes from the State-Of-The-Technology: DNSSEC	x											
3152	BCP	Obsolete	Delegation of IP6.ARPA				x								
3197	Informational		Applicability Statement for DNS MIB Extensions	x			x								
3225	Proposed		Indicating Resolver Support of DNSSEC		x							x			x
3226	Proposed		DNSSEC and IPv6 A6 aware server/resolver message size requirements		x						x	x			
3258	Informational		Distributing Authoritative Name Servers via Shared Unicast Addresses				x								
3363	Informational		Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)					x							
3364	Informational		Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6)	x											

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
3403	Proposed		Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database				x				x	x			
3425	Proposed		Obsoleting IQUERY		x						x	x			
3445	Proposed	Obsolete	Limiting the Scope of the KEY Resource Record (RR)					x							x
3467	Informational		Role of the Domain Name System (DNS)	x											
3490	Proposed	Obsolete	Internationalizing Domain Names in Applications (IDNA)	x		x									
3491	Proposed	Obsolete	Nameprep: A Stringprep Profile for Internationalized Domain Names (IDN)	x		x									
3492	Proposed		Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)	x		x									
3596	Draft		DNS Extensions to Support IP Version 6					x							
3597	Proposed		Handling of Unknown DNS Resource Record (RR) Types					x			x	x			
3645	Proposed		Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)		x						x	x			
3655	Proposed	Obsolete	Redefinition of DNS Authenticated Data (AD) bit	x							x	x			x
3658	Proposed	Obsolete	Delegation Signer (DS) Resource Record (RR)					x			x	x			x
3696	Informational		Application Techniques for Checking and Transformation of Names			x									
3755	Proposed	Obsolete	Legacy Resolver Compatibility for Delegation Signer (DS)		x			x				x			x
3757	Proposed	Obsolete	Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag					x							x
3833	Informational		Threat Analysis of the Domain Name System (DNS)	x											
3845	Proposed	Obsolete	DNS Security (DNSSEC) NextSECure (NSEC) RDATA Format					x							x
3901	BCP		DNS IPv6 Transport Operational Guidelines				x								
4025	Proposed		A Method for Storing IPsec Keying Material in DNS					x							
4033	Proposed		DNS Security Introduction and Requirements	x											x

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
4034	Proposed		Resource Records for the DNS Security Extensions					x							x
4035	Proposed		Protocol Modifications for the DNS Security Extensions		x						x	x			x
4074	Informational		Common Misbehavior Against DNS Queries for IPv6 Addresses								x				
4159	BCP		“Deprecation of “ip6.int”	x			x								
4185	Informational		National and Local Characters for DNS Top Level Domain (TLD) Names	x											
4255	Proposed		Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints					x							
4339	Informational		IPv6 Host Configuration of DNS Server Information Approaches	x											
4343	Proposed		Domain Name System (DNS) Case Insensitivity Clarification			x					x	x			
4367	Informational		What’s in a Name: False Assumptions about DNS Names	x											
4398	Proposed		Storing Certificates in the Domain Name System (DNS)					x							
4408	Experimental		Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1					x							
4431	Informational		The DNSSEC Lookaside Validation (DLV) DNS Resource Record					x							x
4470	Proposed		Minimally Covering NSEC Records and DNSSEC On-line Signing				x				x				x
4471	Experimental		Derivation of DNS Name Predecessor and Successor			x									
4472	Informational		Operational Considerations and Issues with IPv6 DNS				x								
4509	Proposed		Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (Rrs)					x							x
4592	Proposed		The Role of Wildcards in the Domain Name System	x							x	x			
4635	Proposed		HMAC SHA TSIG Algorithm Identifiers							x	x	x			
4641	Informational	Obsolete	DNSSEC Operational Practices				x								x
4697	BCP		Observed DNS Resolution Misbehavior									x			

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
4701	Proposed		A DNS Resource Record (RR) for Encoding Dynamic Host Configuration Protocol (DHCP) Information (DHCID RR)					x							
4892	Informational		Requirements for a Mechanism Identifying a Name Server Instance	x											
4955	Proposed		DNS Security (DNSSEC) Experiments	x											x
4956	Experimental		DNS Security (DNSSEC) Opt-In		x			x			x	x		x	x
4986	Informational		Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover	x											
5001	Proposed		DNS Name Server Identifier (NSID) Option		x						x	x			
5011	Standard		Automated Updates of DNS Security (DNSSEC) Trust Anchors				x	x				x			x
5074	Informational		DNSSEC Lookaside Validation (DLV)									x			x
5155	Proposed		DNS Security (DNSSEC) Hashed Authenticated Denial of Existence					x			x	x			x
5205	Experimental		Host Identity Protocol (HIP) Domain Name System (DNS) Extension					x							
5358	BCP		Preventing Use of Recursive Nameservers in Reflector Attacks				x					x			
5395	BCP	Obsolete	Domain Name System (DNS) IANA Considerations	x											
5452	Proposed		Measures for Making DNS More Resilient against Forged Answers							x		x			
5507	Informational		Design Choices When Expanding the DNS	x											
5625	BCP		DNS Proxy Implementation Guidelines						x						
5702	Proposed		Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC					x							x
5855	BCP		Nameservers for IPv4 and IPv6 Reverse Zones				x								
5864	Proposed		DNS SRV Resource Records for AFS					x							
5890	Proposed		Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework	x		x									
5891	Proposed		Internationalized Domain Names for Applications (IDNA): Protocol	x		x									

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
5933	Proposed		Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC					x							x
5936	Proposed		DNS Zone Transfer Protocol (AXFR)										x		
5966	Proposed		DNS Transport over TCP – Implementation Requirements		x						x	x			
6014	Proposed		Cryptographic Algorithm Identifier Allocation for DNSSEC	x											x
6147	Proposed		DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers	x							x	x			
6168	Informational		Requirements for Management of Name Servers for the DNS	x			x								
6195	BCP	Obsolete	Domain Name System (DNS) IANA Considerations	x											
6303	BCP		Locally Served DNS Zones									x			
6304	Informational		AS112 Nameserver Operations				x								
6305	Informational		I'm Being Attacked by PRISONER.IANA.ORG!				x								
6335	BCP		Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry	x											
6563	Informational		Moving A6 to Historic Status					x							
6604	Proposed		xNAME RCODE and Status Bits Clarification		x						x	x			
6605	Proposed		Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC					x							x
6672	Proposed		DNAME Redirection in the DNS					x			x	x			
6698	Proposed		The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA					x							
6725	Proposed		DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates	x											
6742	Experimental		DNS Resource Records for the Identifier-Locator Network Protocol (ILNP)	x		x		x							
6761	Proposed		Special-Use Domain Names	x			x								
6781	Informational		DNSSEC Operational Practices, Version 2				x								x

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
6804	Historic	Historic	DISCOVER: Supporting Multicast DNS Queries	x											
6840	Proposed		Clarifications and Implementation Notes for DNS Security (DNSSEC)								x	x			x
6841	Informational		A Framework for DNSSEC Policies and DNSSEC Practice Statements				x								x
6844	Proposed		DNS Certification Authority Authorization (CAA) Resource Record					x							
6891	Standard		Extension Mechanisms for DNS (EDNS(0))		x						x	x			
6895	BCP		Domain Name System (DNS) IANA Considerations	x											
6912	Informational		Principles for Unicode Code Point Inclusion in Labels in the DNS	x											
6944	Proposed		Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status	x											
6975	Proposed		Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)	x						x		x			x
7043	Informational		Resource Records for EUI-48 and EUI-64 Addresses in the DNS					x							
7085	Informational		Top-Level Domains That Are Already Dotless	x		x	x								
7218	Standard		Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)	x											
7314	Informational		Extension Mechanisms for DNS (EDNS) EXPIRE Option		x										
7344	Informational		Automating DNSSEC Delegation Trust Maintenance		x		x	x							x
7477	Standard		Child-to-Parent Synchronization in DNS				x	x			x				
7534	Informational		AS112 Nameserver Operations				x								
7535	Informational		AS112 Redirection Using DNAME				x								
7583	Informational		DNSSEC Key Rollover Timing Considerations								x				x
7626	Informational		DNS Privacy Considerations	x											
7646	Informational		Definition and Use of DNSSEC Negative Trust Anchors	x			x								x

RFC	Type	Status	Title	Bgnd	Prot	Names	Ops	RR	Proxy	Stub	Auth	Res	Xfr	DDNS	DNSSEC
7671	Standard		The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance	x			x	x							
7686	Standard		The ".onion" Special-Use Domain Name	x			x								
7706	Informational		Decreasing Access Time to Root Servers by Running One on Loopback	x			x	x							
7719	Informational		DNS Terminology	x											
7766	Standard		DNS Transport over TCP – Implementation Requirements	x											

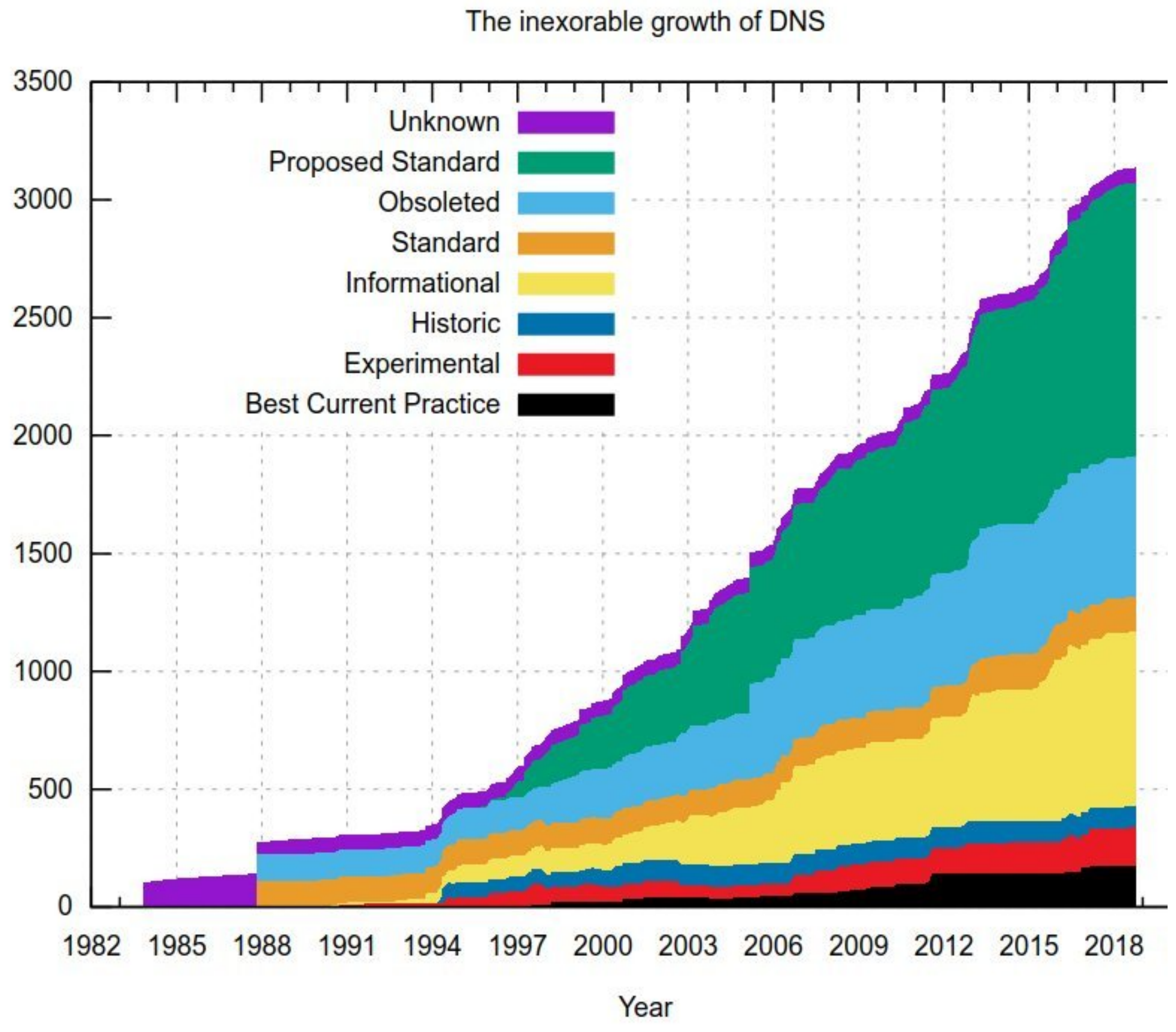
RFC 7793 *(was draft-ietf-dnsop-rfc6598-rfc6303)* **Adding 100.64.0.0/10 Prefixes to the IPv4 Locally-Served DNS Zones Registry**	2016-05 6 pages	Best Current Practice RFC
RFC 7816 *(was draft-ietf-dnsop-qname-minimisation)* **DNS Query Name Minimisation to Improve Privacy** Errata	2016-03 11 pages	Experimental RFC
RFC 7828 *(was draft-ietf-dnsop-edns-tcp-keepalive)* **The edns-tcp-keepalive EDNS0 Option**	2016-04 11 pages	Proposed Standard RFC
RFC 7871 *(was draft-ietf-dnsop-edns-client-subnet)* **Client Subnet in DNS Queries** Errata	2016-05 30 pages	Informational RFC
RFC 7873 *(was draft-ietf-dnsop-cookies)* **Domain Name System (DNS) Cookies**	2016-05 25 pages	Proposed Standard RFC
RFC 7901 *(was draft-ietf-dnsop-edns-chain-query)* **CHAIN Query Requests in DNS**	2016-06 16 pages	Experimental RFC
RFC 8020 *(was draft-ietf-dnsop-nxdomain-cut)* **NXDOMAIN: There Really Is Nothing Underneath**	2016-11 10 pages	Proposed Standard RFC
RFC 8027 *(was draft-ietf-dnsop-dnssec-roadblock-avoidance)* **DNSSEC Roadblock Avoidance** Errata	2016-11 19 pages	Best Current Practice RFC
RFC 8078 *(was draft-ietf-dnsop-maintain-ds)* **Managing DS Records from the Parent via CDS/CDNSKEY** Errata	2017-03 10 pages	Proposed Standard RFC
RFC 8109 *(was draft-ietf-dnsop-resolver-priming)* **Initializing a DNS Resolver with Priming Queries**	2017-03 7 pages	Best Current Practice RFC
RFC 8145 *(was draft-ietf-dnsop-edns-key-tag)* **Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)**	2017-04 13 pages	Proposed Standard RFC Updated by RFC8553
RFC 8198 *(was draft-ietf-dnsop-nsec-aggressiveuse)* **Aggressive Use of DNSSEC-Validated Cache**	2017-07 13 pages	Proposed Standard RFC
RFC 8244 *(was draft-ietf-dnsop-sutld-ps)* **Special-Use Domain Names Problem Statement**	2017-10 25 pages	Informational RFC
RFC 8482 *(was draft-ietf-dnsop-refuse-any)* **Providing Minimal-Sized Responses to DNS Queries That Have QTYPE=ANY**	2019-01 10 pages	Proposed Standard RFC
RFC 8490 *(was draft-ietf-dnsop-session-signal)* **DNS Stateful Operations**	2019-03 64 pages	Proposed Standard RFC Updated by RFC7766
RFC 8499 *(was draft-ietf-dnsop-terminology-bis)* **DNS Terminology**	2019-01 50 pages	Best Current Practice RFC
RFC 8501 *(was draft-ietf-dnsop-isp-ip6rdns)* **Reverse DNS in IPv6 for Internet Service Providers**	2018-11 15 pages	Informational RFC
RFC 8509 *(was draft-ietf-dnsop-kskroll-sentinel)* **A Root Key Trust Anchor Sentinel for DNSSEC**	2018-12 19 pages	Proposed Standard RFC
RFC 8552 *(was draft-ietf-dnsop-attrleaf)* **Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves** Errata	2019-03 15 pages	Best Current Practice RFC
RFC 8553 *(was draft-ietf-dnsop-attrleaf-fix)* **DNS Attrleaf Changes: Fixing Specifications That Use Underscored Node Names**	2019-03 15 pages	Best Current Practice RFC

Active Internet-Drafts (13 hits)		
draft-ietf-dnsop-7706bis-03 **Running a Root Server Local to a Resolver**	2019-03-07 13 pages	I-D Exists WG Document: Informational
draft-ietf-dnsop-algorithm-update-10 **Algorithm Implementation Requirements and Usage Guidance for DNSSEC**	2019-04-20 11 pages	RFC Ed Queue : RFC-EDITOR for 35 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir
draft-ietf-dnsop-alt-tld-11 **The ALT Special Use Top Level Domain**	2019-01-09 11 pages	I-D Exists Held by WG: Proposed Standard
draft-ietf-dnsop-aname-03 **Address-specific DNS aliases (ANAME)**	2019-04-15 15 pages	I-D Exists WG Document: Proposed Standard
draft-ietf-dnsop-dns-capture-format-10 **C-DNS: A DNS Packet Capture Format**	2018-12-12 77 pages	RFC Ed Queue : EDIT for 143 days Submitted to IESG for Publication: Proposed Standard Reviews: genart, opsdir, secdir
draft-ietf-dnsop-dns-tcp-requirements-03 **DNS Transport over TCP - Operational Requirements**	2019-01-02 21 pages	I-D Exists WG Document: Best Current Practice
draft-ietf-dnsop-extended-error-05 **Extended DNS Errors**	2019-03-11 15 pages	I-D Exists In WG Last Call
draft-ietf-dnsop-multi-provider-dnssec-01 **Multi Provider DNSSEC models**	2019-03-11 12 pages	I-D Exists WG Document: Informational
draft-ietf-dnsop-no-response-issue-13 **A Common Operational Problem in DNS Servers - Failure To Communicate.**	2019-02-25 26 pages	I-D Exists WG Document: Best Current Practice
draft-ietf-dnsop-rfc2845bis-03 **Secret Key Transaction Authentication for DNS (TSIG)**	2019-03-07 26 pages	I-D Exists WG Document: Internet Standard
draft-ietf-dnsop-rfc7816bis-02 **DNS Query Name Minimisation to Improve Privacy**	2019-03-23 13 pages	I-D Exists WG Document: Internet Standard
draft-ietf-dnsop-serve-stale-05 **Serving Stale Data to Improve DNS Resiliency**	2019-04-16 12 pages	I-D Exists WG Document
draft-wessels-dns-zone-digest-06 **Message Digest for DNS Zones**	2019-02-13 27 pages	I-D Exists Adopted by a WG: Experimental

Aktivní Internetové Drafty (I-D)

DNS je jednoduché!

- Přibližně 200 RFC
- Přibližně 3000 stránek
- Přibližně **milión** slov



Graph by Bert Hubert @ PowerDNS

Co s tím?

- Přestat psát nová RFC
- Konsolidovat stará RFC
  - RFC1034, RFC1035, RFC1912, RFC2181
  - Přepsat do „moderního“ jazyka
  - Poslední dobrovolník ⟹⟹⟹
- Vyžadovat implementace v DNS serverech před plnou standardizací

Photo by David Clode on Unsplash

„Novinky“ v DNS

- DNS Query Name Minimization
    - RFC 7816
    - draft-ietf-dnsop-rfc7816bis-02
- DNS Cookies
    - RFC 7858
    - draft-sury-toorop-dns-cookies-algorithms
- DNS over TLS
    - RFC 7858, RFC 8310
    - Padding - RFC 7830, RFC 8467
- DNS over HTTPS
    - RFC 8484
- ANAME
    - draft-hunt-dnsop-aname

Query Name Minimization

- Tradiční DNS posílá zbytečně moc informací
- Součást „DNS Privacy“
- QNAME Minimization omezuje informace z DNS dotazů na nezbytné minimum

Photo by Craig McLachlan on Unsplash

Query Name Minimization

- Tradiční DNS

```
QTYPE QNAME         TARGET
A     www.isc.org.  root nameserver
A     www.isc.org.  .org nameserver
A     www.isc.org.  isc.org. ns
```

Query Name Minimization

- Tradiční DNS

```
QTYPE QNAME          TARGET
A     www.isc.org.  root nameserver
A     www.isc.org.  .org nameserver
A     www.isc.org.  isc.org. ns
```

- Aggressive QNAME-Min

```
QTYPE QNAME          TARGET
NS    org.           root nameserver
NS    isc.org.       .org nameserver
NS    www.isc.org.  isc.org nameser.
A     www.isc.org.  isc.org nameser.
```

QNAME Minimization & The Internet

- Load-Balancery, CDN
  - DNS je jednoduché, že?
  - Neodpovídají na ‚NS‘, jen na ‚A‘
  - NXDOMAIN pro Empty Non-Terminal
    - www.cdn.example.com
    - A cdn.example.com -> NXDOMAIN
    - Správně: NODATA
    - Viz RFC 8020 - NXDOMAIN: There Really Is Nothing Underneath

Photo by mwangi gatheca on Unsplash

Query Name Minimization

- Tradiční DNS

```
QTYPE QNAME         TARGET
A     www.isc.org.  root nameserver
A     www.isc.org.  .org nameserver
A     www.isc.org.  isc.org. ns
```

- Aggressive QNAME-Min

```
QTYPE QNAME         TARGET
NS    org.          root nameserver
NS    isc.org.      .org nameserver
NS    www.isc.org.  isc.org nameser.
A     www.isc.org.  isc.org nameser.
```

- Relaxed QNAME-Min

```
QTYPE QNAME          TARGET
A     _.org.          root nameserver
A     _.isc.org.      .org nameserver
A     _.www.isc.org. isc.org nmsrv.
A.    www.isc.org.   isc.org nameser.
```

- Relaxed QNAME-Min

```
QTYPE QNAME            TARGET
NS    example.         root ns
NS    cdn.example.     .example ns
-> SERVFAIL/REFUSED/NXDOMAIN
A     www.cdn.example. .example ns
```

Query Name Minimization

- BIND 9.14
  - Relaxed mode by default

```
options {
    qname-mininization <disabled|relaxed|strict>;
}
```

- Knot Resolver
  - Relaxed mode by default

```
option(NO_MINIMIZE, <true|false>)
```

Unbound

  - Relaxed mode by default

```
qname-minimisation: <yes|no>
qname-minimisation-strict: <yes|no>
```

DNS Cookies

- Přidavá do DNS dotazů a odpovědí „Cookie“
  - Ochrana proti podvrženým DNS zprávám
- DNS Client pošle „Client Cookie“ (nonce):
  - Client IP address
  - Server IP address
  - Client Secret (náhodný při startu serveru)
- DNS Server vypočítá „Server Cookie“ z:
  - Client Cookie
  - Timestamp
  - Server Secret (náhodný nebo nakonfigurovaný)
  - …další hodnoty

Photo by Emily Wilson on Unsplash

DNS Cookies v Anycastu

- BIND implementuje následující algoritmy:
  - FNV
  - HMAC-SHA256-64
  - AES
- Knot DNS implementuje následující algoritmy
  - SipHash 2-4

DNS Cookie Algoritmy (draft)

- Společná práce ISC a NlNetLabs s přispěním CZ.NIC a dalších
- Místo hashovací funkce se použije pseudo-random funkce SipHash 2-4
- Server Cookie obsahuje:
  - Verzi (8 bitů)
  - Algoritmus (8 bitů)
  - Rezervované pole (16 bitů
  - Timestamp (32 bitů)
  - Výstup z SipHash 2-4 (64 bitů)

RFC 7858 - DNS over TLS

- Další součást „DNS Privacy“
- Šifrování na transportní vrstvě
- Zatím jen stub ⟷ resolver
- Vlastní port - 853
- DoT Usage Policies
  - Strict (Authentication + Encryption)
  - Opportunistic
- Authentication
  - SPKI Pinning
  - Authentication Domain Name
  - ADN via DANE
  - DHCP

RFC 7830 - EDNS(0) Padding

- DNS zprávy jsou poměrně krátké
- DNS over TLS zprávy se liší podle velikosti obsahu → délka může prozradit obsah
- EDNS(0) Padding přidává do DNS zprávy vycpávku, která unifikuje délku „na drátě“
- RFC 8467 doporučuje zarovnávat zprávy na násobky 128 oktetů (bajtů)

Photo by Trym Nilsen on Unsplash

RFC 8484 - DNS over HTTPS

- HTTP(s) je transportní vrstva
- Data jsou v DNS wire formátu
- Umožňuje míchání různých dat v jednom streamu
- DNS je pro on-path útočníka „neviditelné“
- Umožňuje cachování na HTTP vrstvě
  - Složitější interakce HTTP (Max-)Age a DNS TTL

ANAME

- Staronový problém
  - Přesměrování z example.com (zone cut) na www.example.com nebo cdn.example.net
  - CNAME+DNAME — draft-sury-dnsext-cname-dname (2010)
    - Experimentálně ověřeno, že funguje pro parent zónu, ale nefunguje pro child zónu (nelze umístit do zone apexu)
  - BNAME — draft-yao-dnsext-bname (2009, 2010)
  - HTTP RR — draft-bellis-dnsop-http-record (2018)
    - Jde na problém oklikou - zavádí záznam pouze pro HTTP (což pokrývá 99,99% problému)
  - Některé DNS hostingy mají vlastní řešení — navzájem nekompatibilní

ANAME

- ANAME — něco jako CNAME, ale jen pro A + AAAA záznamy
  - Podporuje transfer mezi různými nameservery a poskytovateli DNS hostingů
  - Největší problém je plynulý přechod a podpora „starých“ DNS klientů
  - Vyžaduje processing na straně primárního autoritativního serveru
    - Získání „sibling address records“ (lokální kopie cílových adres), jejich podepsání a transfer na sekundární NS
  - Volitelně vyžaduje processing na straně resolverů a DNS clientů (pokud chtějí validovat cílové adresy)
  - Funguje i s DNSSEC, ale vyžaduje online podepisování nebo podporu ANAME na straně klientů

Photo by Emily Morter on Unsplash