TLD Apex History Data Dictionary

2022-03-23 Edition

The TLD Apex History is a summary history of DNSSEC-related records observed at the apex of TLD zones. The summary history is made available in both CSV and JSON.

This document explains the meanings and syntax used for the fields in the summary history table. For CSV, these are the column names that appear in the first line of a csv file. For JSON, these are the field selector names.

General Column Rules

All data is represented in the files as strings, UTF-8, although only ASCII characters appear.

Each record in the table represents a string of dates a particular record was observed. What specifies "a particular record" is dependent on the resource record type. For an SOA Resource Record, the RNAME and MNAME fields define this, the other fields are ignored. For an RRSIG Resource Record, the signature duration (calculated from the expiry and inception times) is not used to differentiate records but is recorded as a varying range.

Where there is no appropriate value, the CSV file will have "" and the JSON file will have null (no quotes).

Each column with a name ending in "_RANGE" contains a set of observed values. These fields begin and end in curly braces, i.e., "{" and "}" with individual values separated by commas. The implication is that these fields ought to be treated as a mathematical set, with no sequencing (in time) nor relative presence (distribution} intended. The significance of these fields is often whether they change or not (such as using RRSIG signature duration jitter) but in some cases patterns indicate other interesting behavior.

Individual Column Definitions

"OWNER"

The "A label" of the TLD in fully-qualified domain name form, using upper-case ASCII characters. (For the sake of matching, recommend using a well-developed DNS-library name comparison routine.)

"RRTYPE"

The mnemonic of the resource record type. See the registry hosted by IANA for Resource Record Types for formatting.

https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4

"FIRST_SEEN"

The YYYY-MM-DD of the date when the record was first observed. The string format may be written in code as '%Y-%m-%d'.

"LAST_SEEN"

The YYYY-MM-DD of the date when the record was last (or most recently) observed. The string format may be written in code as '%Y-%m-%d'.

From "FIRST_SEEN" to "LAST_SEEN", inclusive, the record was observed. If FIRST and LAST are the same value, the record was seen just the one day. In other words the number of days a record was seen is (LAST-SEEN - FIRST_SEEN +1).

"NS_NSDNAME"

If RRTYPE is NS this is the target name of the record. Otherwise, empty in CSV, null in JSON.

"SOA_MNAME"

If RRTYPE is SOA this is the MNAME field. (See: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION.)

"SOA_RNAME"

If RRTYPE is SOA this is the RNAME field. (See: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION.)

"DNSKEY_ROLE"

If RRTYPE is DNSKEY this field is either "ZONE", "SEP", "R-S" or "R-Z", based on the flags field of the DNSKEY Resource Record.

"DNSKEY_PROTOCOL"

If the RRTYPE is DNSKEY this field is always "DNSSEC" due to the field's definition being frozen in the specification.

"DNSKEY_DNSSEC_SECURITY_ALGORITHM"

If the RRTYPE is DNSKEY this field is a non-standard mnemonic for the value in the algorithm field. The non-standard mnemonics in use are in the third column.

DNSSEC Security Algorithm	IANA Mnemonic	TLD APEX
5	RSASHA1	RSA-SHA1
7	RSASHA1-NSEC3-SHA1	RSA-SHA1-N
8	RSASHA256	RSA-SHA256
10	RSASHA512	RSA-SHA512
13	ECDSAP256SHA256	ECDSA256SH
14	ECDSAP384SHA384	ECDSA384SH

"DNSKEY_KEYLEN"

If the RRTYPE is DNSKEY the number of bits in the key, expressed in string form.

"DNSKEY_KEYTAG"

If the RRTYPE is DNSKEY the keytag of the key, expressed in string form padded with leading 0's to five characters.

"DNSKEY_EXPLEN"

If the RRTYPE is DNSKEY and the key is RSA this is an assessment of the length of the exponent. This parameter received attention for a short time early in DNSSEC deployment, once software bugs were addressed, interest in this waned and became a forgotten or neglected column.

Field Value	Length of exponent	Notes
SMALL	1	
LARGE	3	
OBESE	5	Triggered a buffer overflow in early code bases
UNKNOWN	some other value	Code did not preserve value
none	not applicable	

"DNSKEY_KEY"

If the RRTYPE is DNSKEY this column contains the base64 encoded public key.

"DNSKEY_TTL_RANGE"

If the RRTYPE is DNSKEY this field contains the set of TTL values observed.

The field is encoded with braces ('{' and '}') surrounding a comma delimited series of values. Each value is encoded as "xdyhzmws" with "d", "h", "m" and "s" representing the time units of days, hours, minutes, and seconds. The values "x", "y", "z" and "w" are between 1 and the appropriate maximum, if any. (For hours, 23, for minutes and seconds, 59.) If a time unit's "prefix" is 0, the time unit is omitted.

For example, 10d3h is 10 days and 3 hours.

"DS_KEYTAG"

If the RRTYPE is DS the keytag of the key indicated by the DS record, expressed in string form, and padded with leading 0's to five characters.

"DS_DNSSEC_SECURITY_ALGORITHM"

If the RRTYPE is DS the DNSSEC security algorithm of the referenced key, using the same values as documented in for DNSKEY_DNSSEC_SECURITY_ALGORITHM.

"DS_HASH_ALGORITHM"

If the RRTYPE is DS the hashing algorithm used to generate the DS digest. The values correspond to the Description column in *DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms*.

https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml#ds-rr-types-1

"DS_DIGEST"

If the RRTYPE is DS this is the base64 encoded digest referencing the intended key.

"NSEC3PARAM_HASH_ALGORITHM"

If the RRTYPE is NSEC3PARAM this is the hashing algorithm used to generate the next hash. The value is either "SHA-1" or empty, as there is no likely additional hashing algorithm to be used by NSEC3. (If there is, consult the appropriate IANA-hosted registry.)

"NSEC3PARAM_FLAGS"

If the RRTYPE is NSEC3PARAM this field is "NoFlags" as no flags are set in the NSEC3PARAM. (If any values are ever set, consult the appropriate registry.)

Note that these flags can change among NSEC3PARAM and NSEC3 records in a zone according to the protocol, but in practice never do. There is no known, distributed software that accommodates different flag settings within a zone.

"NSEC3PARAM_ITERATIONS"

If the RRTYPE is NSEC3PARAM this is the number of iterations used. The field is numeric, expressed as a string.

"NSEC3PARAM_SALT"

If the RRTYPE is NSEC3PARAM this is the hex-encoded salt used by NSEC3.

"RRSIG_TYPE_COVERED"

If the RRTYPE is RRSIG this is the type covered value for the signature. The formatting of this field is the same as the formatting for RRTYPE.

"RRSIG_DNSSEC_SECURITY_ALGORITHM"

If the RRTYPE is RRSIG this is the DNSSEC security algorithm for the signature, using the same values as documented in for DNSKEY_DNSSEC_SECURITY_ALGORITHM.

"RRSIG_SIGNER"

If the RRTYPE is RRSIG this is a fully qualified (alabel) domain name, lower case owning the public key used for validation.

"RRSIG_KEYTAG"

If the RRTYPE is RRSIG this is the keytag of the public key used for validation, expressed in string form, and padded with leading 0's to five characters.

"RRSIG_DURATION_RANGE"

If the RRTYPE is RRSIG this is the set of signature durations (signature expiration time minus signature inception time) observed for RRSIG resource records matching the public key and the type covered. (A signature may be regenerated and the record updated, but this change is not considered to be a different record.)

The field is encoded with braces ('{' and '}') surrounding a comma delimited series of values. Each value is encoded as "xwyd" with "w" and "d" representing the time units of weeks and days. The values "x" is 1 or more (no leading 0), and the values of "y" are between 1 and 6. If a time unit's "prefix" is 0, the time unit is omitted.

For example, 3w2d is 3 weeks and 2 days, another example, 5w is 5 weeks.

"RRSIG_TTL_RANGE"

If the RRTYPE is RRSIG this is the set of TTL values for the RRSIG record.

The field is encoded with braces ('{' and '}') surrounding a comma delimited series of values. Each value is encoded as "xdyhzmws" with "d", "h", "m" and "s" representing the time units of days, hours, minutes, and seconds. The values "x", "y", "z" and "w" are between 1 and the appropriate maximum, if any. (For hours, 23, for minutes and seconds, 59.) If a time unit's "prefix" is 0, the time unit is omitted.

For example, 10d3h is 10 days and 3 hours.

Contact information

Questions, suggestions regarding this (version of the) data dictionary ought to be sent to edward.lewis@icann.org.