Explanation of the Status Codes that can appear in the DANE Error Report

A domain name **only** appears in the report if – according to the rules of the DNS Resilience Programme – an **erroneous or non-compliant configuration for DANE** has been detected on that day.
A domain name **does not** appear in the report if **no TLSA records** for port 25 TCP could be detected or if measurement was not possible on that day (timeout etc.).

Many status codes are composites of two or more codes.

The DANE assessment combines data from two separate measurements. The MX and TLSA records are measured on the same day but not at the same time. This means it cannot be guaranteed that the MX records remain unchanged by the time the TLSA measurements are done.

Error date: Date of measurement
DANE SC: Status Code for DANE (composite)
DANE Comp: Components of the composite code
Report URL Template: Base URL of dashboard, add domain name to find more details

Base Status Codes

2 – NXDOMAIN. Will co-appear with other status codes to indicate that an NXDOMAIN was encountered.

4 – SERVFAIL. Will co-appear with other status codes to indicate that a SERVFAIL was encountered.

8 – TIMEOUT. Will co-appear with other status codes to indicate that a TIMEOUT was encountered.

MX Status Codes

32 – "Null" MX record. The domain name has a single **MX** record, and it is set to the "no service" record as defined in RFC7505. This status code is informational and should not be considered an error or warning on its own. If it appears with other status codes (e.g. with status code 64) the configuration may be faulty.

64 – Invalid or missing DNSSEC signature for at least one MX record. Note that also "null" **MX** records as defined in RFC 7505 need to be DNSSEC secured.

TLSA Status Codes

128 – Missing TLSA record(s). The measuring system could not find at least one **TLSA** record for all **MX** records at the domain apex. May co-appear with the NXDOMAIN (2), SERVFAIL (4), or TIMEOUT (8) codes.

256 – Invalid or missing DNSSEC signature for at least one TLSA record.

512 – Prohibited certificate usage. One or more of the **TLSA** records has its certificate usage field set to a value other than DANE-TA [2] or DANE-EE [3].

1024 – Prohibited selector. One of more of the **TLSA** records has its selector set to a value other than Cert [0] or SPKI [1].

2048 – Prohibited matching type. One or more of the **TLSA** records has its matching type set to a value other than SHA-256 digest [1] or SHA-512 digest [2].

4096 – Invalid TLSA record(s). A published **TLSA** record is not compliant with RFC7671. The **TLSA** record uses out of spec RFC7671 configuration values:

- *Certificate Usage* should be one of the values [0, 1, 2, 3, 255]
- *Selector* should be one of the values [0, 1, 255]
- *Matching Type* should be one of the values [0, 1, 2, 255]
- *Certificate Association Data*, depending on the *Matching Type*:
  - 0 Full match: depending on *Selector*:
    - 0: Valid Certificate binary structure [RFC5280]
    - 1: Valid *SubjectPublicKeyInf*o DER-encoded binary structure [RFC5280]
  - 1 SHA-256: 256 bits hash in hexadecimal
  - 2 SHA-512: 512 bits hash in hexadecimal