

MLCerts Paper Auxiliary Material

1 Implementing Transcert and Frankencerts

We used the source released by the authors for Transcert and Frankencerts implementations. We used “Transcert_0 (30K)”, the authors’ best model (1.43x NEZHA, 10x RFCcerts, 18x Frankencerts) with their parameters: 1,005 seeds to generate 30k certificates. For Frankencerts, we used 100K seeds to generate 8M certificates, as done by the authors. During testing, we used the same environment as for MLCerts (Zmap seeds, libraries, simulated time).

2 ZLint Errors

Listing 1 shows the list of ZLint Errors triggered by discrepancy-producing certificates, that are *not* triggered when using either Transcert or Frankencerts. We sent our disclosures for a smaller set of 22 errors (instead of 24) because we excluded errors triggered by real-world certificates (IPv4).

3 Meaningful Information from Output Logs

To gain meaningful information from the output logs of TLS libraries in our security evaluation, we analyze the unique strings for all certificate validations. We identify the security-relevant strings in Listing 2, which we use to analyze the discrepancy-producing certificates in Section 5.3.

4 Old Library Versions

During our research, we updated the versions of the TLS libraries that we analyze. The older versions of the libraries for which we sent disclosure notifications and received acknowledgements are listed in Table 1. All behaviors reported in our paper are for the recent versions of libraries, reported in Table 2.

Table 1: TLS libraries used earlier in our research.

Library	Version	Release Date
OpenSSL	1.1.1t (LTS)	7 Feb 2023
MbedTLS	3.3.0	14 Dec 2022
GnuTLS	3.6.16 (LTS)	24 May 2021
LibreSSL	3.6.2	7 Feb 2023
MatrixSSL	4.6.0	29 Dec 2022

Table 2: TLS libraries used for results in our paper.

Library	Version	Release Date
OpenSSL	3.3.2	03 Sep 2024
MbedTLS	3.6.1	30 Aug 2024
GnuTLS	3.7.11	27 May 2024
LibreSSL	3.9.2	12 May 2024
MatrixSSL	4.6.0	29 Dec 2022

```
e_dnsname_hyphen_in_sld
e_ext_cert_policy_disallowed_any_policy_qualifier
e_ext_cert_policy_duplicate
e_ext_ian_dns_not_ia5_string
e_ext_ian_uri_format_invalid
e_ext_ian_uri_host_not_fqdn_or_ip
e_ext_ian_uri_relative
e_ext_san_dns_not_ia5_string
e_ext_san_rfc822_format_invalid
e_ian_wildcard_not_first
e_international_dns_name_not_unicode
e_name_constraint_empty
e_path_len_constraint_zero_or_less
e_public_key_type_not_allowed
e_san_dns_name_includes_null_char
e_serial_number_longer_than_20_octets
e_serial_number_not_positive
e_spki_rsa_encryption_parameter_not_null
e_sub_cert_postal_code_must_not_appear
e_sub_cert_street_address_should_not_exist
e_subject_organization_name_max_length
e_subject_postal_code_max_length
e_subject_surname_max_length
e_tbs_signature_rsa_encryption_parameter_not_null
```

Listing 1: Unique ZLint errors triggered by discrepancy-producing certificates.

```

# GnuTLS
"signature in the certificate is invalid",
"certificate chain uses insecure algorithm",
"certificate issuer is unknown",
"certificate chain uses expired certificate",
"Error in the time fields of certificate",
"Duplicate extension in X.509 certificate",
"certificate chain violates the signer's constraints",
"certificate chain uses not yet valid certificate",
"certificate contains an unknown critical extension",

# LibreSSL
"certificate signature failure",
"unable to get local issuer certificate",
"unsupported or invalid name syntax",
"certificate has expired",
"EE certificate key too weak",
"certificate is not yet valid",
"unhandled critical extension",
"bad signature",
"invalid time format",
"no subject details",
"wrong signature length",
"unknown message digest algorithm",
"unknown signature algorithm",
"Unspecified certificate verification error",
"invalid or inconsistent certificate policy extension"

# MbedTLS
"certificate is not correctly signed by the trusted CA",
"certificate is signed with an unacceptable hash",
"certificate validity has expired",
"certificate validity starts in the future",

# MatrixSSL
"FAIL Auth Key / Subject Key Match",
"FAIL Distinguished Name Match",
"Assertion `faildate == 0' failed",
"unsupported critical extension was encountered",
"End-entity certificate not for TLS usage",

# OpenSSL
"certificate signature failure",
"bad signature",
"certificate has expired",
"format error in certificate's notBefore field",
"format error in certificate's notAfter field",
"certificate is not yet valid",
"unhandled critical extension",
"unknown message digest algorithm",

```

Listing 2: Security-relevant strings in library output logs.