

On the hunt for usable error documentation

What do the developers think?



Technical Writers Workshop Prague

5. 10. 2020

CRCS

Centre for Research on
Cryptography and Security

Martin Ukrop, mukrop@mail.muni.cz

Masaryk University, Czech Republic

Ph.D. research cooperation with Red Hat Czech



- [✉](#)
- [f](#)
- [🐦](#)
- [📧](#)
- [📺](#)
- [🐙](#)

DEVCONF.cz

open source community conference

January 24-26, 2020
Brno, Czech Republic



Connection is secure x

devconf.info/cz/

Connection is secure

- Certificate (Valid)
- Cookies (3 in use)
- Site settings



CONF.cz

open source community conference

January 24-26, 2020
Brno, Czech Republic





Your connection is not private

Attackers might be trying to steal your information from **sha1-intermediate.badssl.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM

- Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Advanced

Back to safety

I need to validate this certificate...

```
[user@devconf ~]$ openssl verify cert.pem
```

I need to validate this certificate...

```
[user@devconf ~]$ openssl verify cert.pem
```

```
C = CZ, ST = Brno, O = DevConf organizers  
error 34 at 0 depth lookup: unhandled critical extension  
error cert.pem: verification failed
```

Google

 openssl unhandled critical extension|



Hľadať Googlom

Skúsím šťastie

X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER

Unable to get CRL issuer certificate.

X509_V_ERR_UNHANDLED_CRITICAL_EXTENSION

Unhandled critical extension.

X509_V_ERR_KEYUSAGE_NO_CRL_SIGN

Key usage does not include CRL signing.

X509_V_ERR_UNHANDLED_CRITICAL_CRL_EXTENSION

Unhandled critical CRL extension.

GNUTLS_CERT_REVOCATION_DATA_ISSUED_IN_FUTURE

The revocation data have a future issue date.

GNUTLS_CERT_SIGNER_CONSTRAINTS_FAILURE

The certificate's signer constraints were violated.

GNUTLS_CERT_MISMATCH

The certificate presented isn't the expected one (TOFU)

GNUTLS_CERT_PURPOSE_MISMATCH

The certificate or an intermediate does not match the intended purpose (extended key usage).

GNUTLS_CERT_MISSING_OCSP_STATUS



_IN_FUTURE

re issue date.

LURE

nts were violated.

re expected one (TOFU)

re does not match the
usage).

And there are MANY possible errors...

X509_V_OK, X509_V_ERR_UNSPECIFIED, X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT, X509_V_ERR_UNABLE_TO_GET_CRL,
X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE, X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE,
X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY, X509_V_ERR_CERT_SIGNATURE_FAILURE,
X509_V_ERR_CRL_SIGNATURE_FAILURE, X509_V_ERR_CERT_NOT_YET_VALID, X509_V_ERR_CERT_HAS_EXPIRED,
X509_V_ERR_CRL_NOT_YET_VALID, X509_V_ERR_CRL_HAS_EXPIRED, X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD,
X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD, X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD,
X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD, X509_V_ERR_OUT_OF_MEM, X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT,
X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN, X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY,
X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE, X509_V_ERR_CERT_CHAIN_TOO_LONG, X509_V_ERR_CERT_REVOKED,
X509_V_ERR_INVALID_CA, X509_V_ERR_PATH_LENGTH_EXCEEDED, X509_V_ERR_INVALID_PURPOSE,
X509_V_ERR_CERT_UNTRUSTED, X509_V_ERR_CERT_REJECTED, X509_V_ERR_SUBJECT_ISSUER_MISMATCH,
X509_V_ERR_AKID_SKID_MISMATCH, X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH, X509_V_ERR_KEYUSAGE_NO_CERTSIGN,
X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER, X509_V_ERR_UNHANDLED_CRITICAL_EXTENSION,
X509_V_ERR_KEYUSAGE_NO_CRL_SIGN, X509_V_ERR_UNHANDLED_CRITICAL_CRL_EXTENSION, X509_V_ERR_INVALID_NON_CA,
X509_V_ERR_PROXY_PATH_LENGTH_EXCEEDED, X509_V_ERR_PROXY_SUBJECT_INVALID,
X509_V_ERR_KEYUSAGE_NO_DIGITAL_SIGNATURE, X509_V_ERR_PROXY_CERTIFICATES_NOT_ALLOWED,
X509_V_ERR_INVALID_EXTENSION, X509_V_ERR_INVALID_POLICY_EXTENSION, X509_V_ERR_NO_EXPLICIT_POLICY,
X509_V_ERR_DIFFERENT_CRL_SCOPE, X509_V_ERR_UNSUPPORTED_EXTENSION_FEATURE, X509_V_ERR_UNNESTED_RESOURCE,
X509_V_ERR_PERMITTED_VIOLATION, X509_V_ERR_EXCLUDED_VIOLATION, X509_V_ERR_SUBTREE_MINMAX,
X509_V_ERR_APPLICATION_VERIFICATION, X509_V_ERR_UNSUPPORTED_CONSTRAINT_TYPE,
X509_V_ERR_UNSUPPORTED_CONSTRAINT_SYNTAX, X509_V_ERR_UNSUPPORTED_NAME_SYNTAX,
X509_V_ERR_CRL_PATH_VALIDATION_ERROR, X509_V_ERR_PATH_LOOP, X509_V_ERR_SUITE_B_INVALID_VERSION,

Writing a better documentation may help...

**But how do we know
what the devs want/need?**

DEVCONF.cz 2020 experiment



DEVCONF.cz 2020 experiment

- Questionnaire on error documentation redesign
 - Current documentation (OpenSSL) and its evaluation
 - Redesigned documentation and its evaluation
 - Ideal documentation opinions
 - Demographics, previous experience

DEVCONF.cz 2020 experiment

- Questionnaire on error documentation redesign
 - Current documentation (OpenSSL) and its evaluation
 - Redesigned documentation and its evaluation
 - Ideal documentation opinions
 - Demographics, previous experience
- Over **180** participants
(*real* devs, admins, ...!)

Original documentation (OpenSSL)

X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER

Unable to get CRL issuer certificate.

X509_V_ERR_UNHANDLED_CRITICAL_EXTENSION

Unhandled critical extension.

X509_V_ERR_KEYUSAGE_NO_CRL_SIGN

Key usage does not include CRL signing.

Redesigned documentation

X509_ERR_UNHANDLED_CRITICAL_EXTENSION

Either critical extension was not recognized, or information in critical extension could not be processed.

Explanation

Certificate extensions can be used for incorporating additional information into a certificate. The extensions can be critical or non-critical. All extensions marked as critical must be processed. If a system, which processes a certificate, cannot recognize a critical extension, it must reject the certificate. It has to reject the certificate also when it recognizes the critical extension, but it cannot process the information contained in the extension.

Security perspective

An extension can carry arbitrary information, and marking it as critical means that it is crucial to process it. If it cannot be processed, there is a security risk that a certificate's key will be used in a manner it must not be, e.g., that a certificate's key will be used for another purpose that it was aimed or that a Certification Authority will issue a certificate for subject name for which it is not allowed to issue certificates, or many other security risks.

What to do

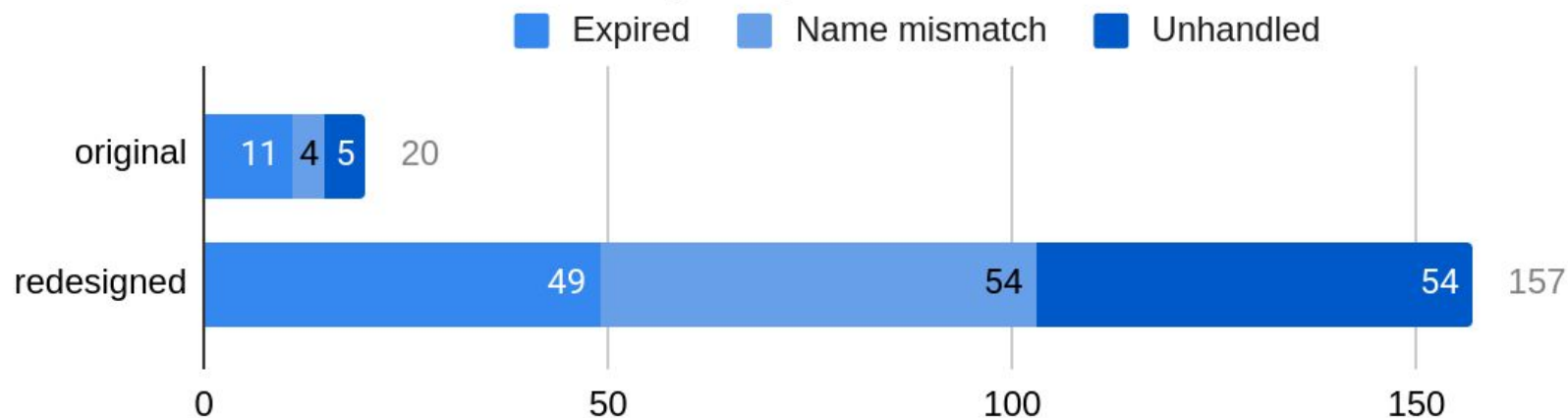
If you are responsible for the certificate, make sure that only necessary extensions are marked as critical and that the values of critical extensions are meaningful. If you are not responsible for the certificate, you can check the critical extensions and the values which contain, but it is not recommended to continue processing the certificate.

Consequences

If you ignore critical extensions that cannot be processed, it may result in unauthorized use of the certificate.

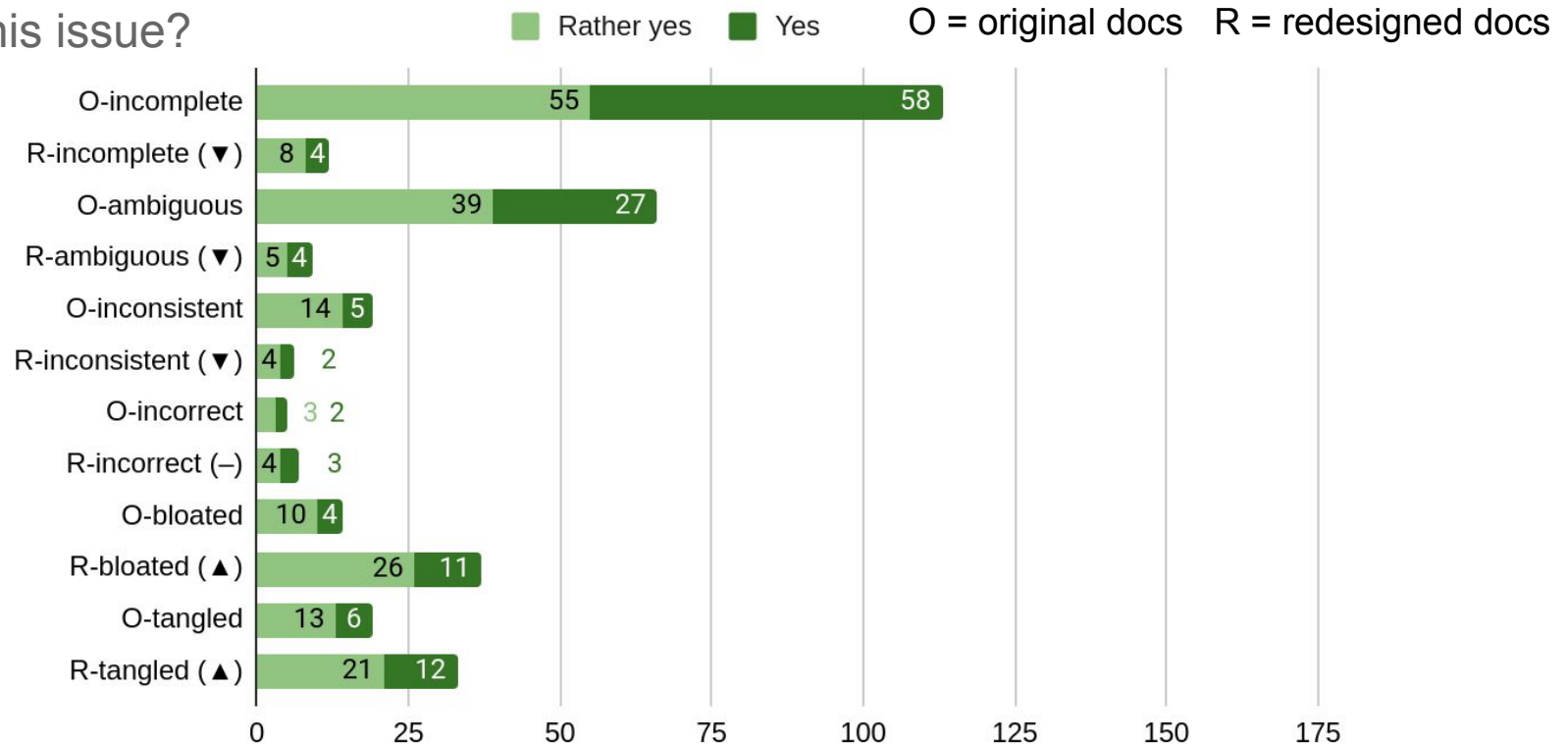
Results sneak peek 1

Which documentation do you prefer?



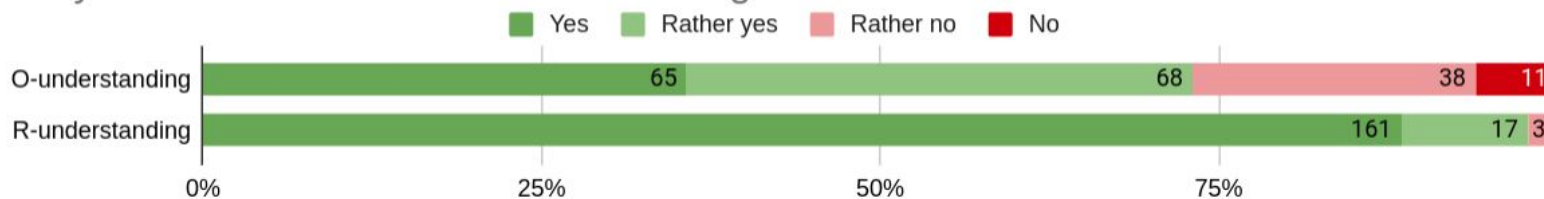
Results sneak peek 2

Does the documentation
have this issue?

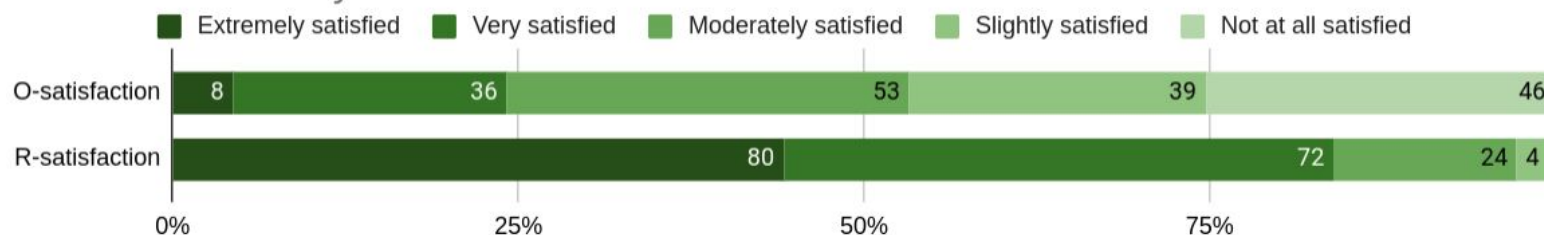


Results sneak peek 3

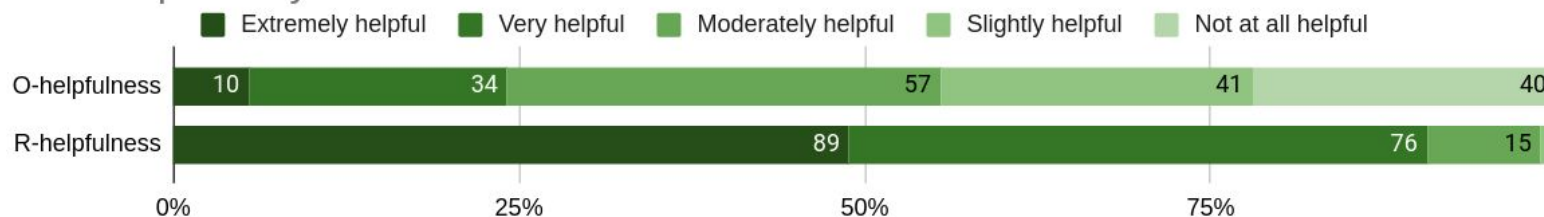
Do you understand the error after reading the documentation?



How satisfied are you with the documentation?

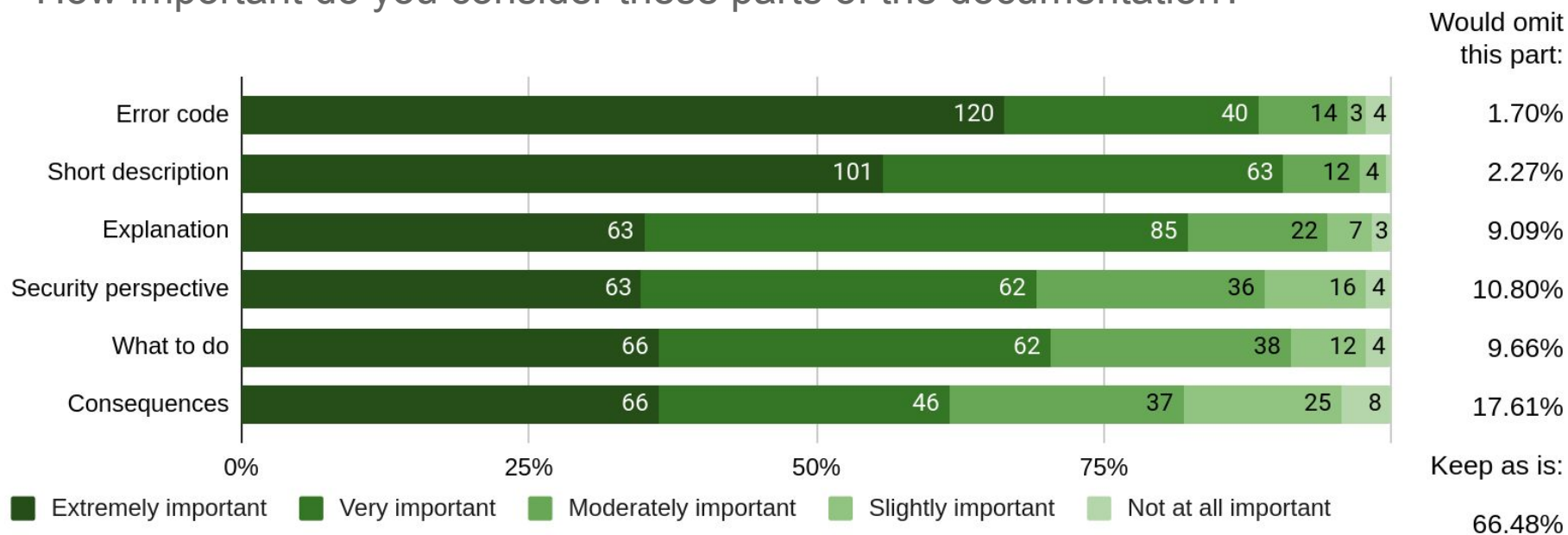


How helpful do you find the documentation?



Results sneak peek 4

How important do you consider these parts of the documentation?



Going further: x509errors.org

- We now “know” what does not work.
- Let’s fix it! (Or at least a bit of it.)

Going further: x509errors.org

- We now “know” what does not work.
- Let’s fix it! (Or at least a bit of it.)
 - Consolidate and map existing errors from multiple libraries
 - Create better documentation

 x509errors.org

Making X.509 errors usable.

Validating X.509 certificates correctly turns out to be pretty complicated (e.g. [Georgiev2012](#)). Yet certificate validation is absolutely crucial for secure communication on the Internet (think [TLS](#)).

Our goal is to simplify the ecosystem by consolidating the errors and their documentation (similarly to [web documentation](#)) and by explaining better what the validation errors mean.


Samples and documentation

For every error, we aim to provide an example certificate (), documentation from OpenSSL () and other libraries ().

We plan to include the error frequency based on IP-wide scans

Multiple libraries

Our consolidated taxonomy aims for eight most used TLS-enabled libraries. The main structure is based on [OpenSSL](#) as it is by far the most used library in the domain of TLS.

 Error mapping

Methodology

We extend the existing research on security, TLS and documentation design. Details are described on a



x509errors.org

Trust or chain related errors

These errors occur when the trust chain to the root certificate is not built correctly or fails.

Relevant links: [Certificate Paths](#) (RFC 5280), [Certificate Revocation Lists](#) (RFC 5280), [OCSP](#) (RFC 2560)

➤ X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT



➤ X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY



➤ X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT



➤ X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN



➤ X509_V_ERR_CERT_CHAIN_TOO_LONG



➤ X509_V_ERR_UNABLE_TO_GET_CRL





➤ X509_V_ERR_UNABLE_TO_GET_CRL_ISSUER

➤ X509_V_ERR_CRL_PATH_VALIDATION_ERROR

▾ X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY



 Example certificate

Download  [the certificate archive](#). If you are interested in generating such certificate yourself, see the generating script for this case on  [the project GitHub](#). To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`


 OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.


 GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND 


The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.



> X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT



> X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN

> X509_V_ERR_CERT_CHAIN_TOO_LONG

 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY    Example certificate

Download  [the certificate archive](#). If you are interested in generating such certificate yourself, see the generating script for this case on  [the project GitHub](#). To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`

 OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.

 GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND 



The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT    X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN X509_V_ERR_CERT_CHAIN_TOO_LONG

▾ X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY
 



 Example certificate

Download  [the certificate archive](#). If you are interested in generating such certificate yourself, see the generating script for this case on  [the project GitHub](#). To get the validation error, run the command as indicated below.

- OpenSSL: `openssl verify endpoint.crt`
- GnuTLS: `certtool --verify --infile endpoint.crt`


 OpenSSL: X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.


 GnuTLS: GNUTLS_CERT_SIGNER_NOT_FOUND 

The certificate's issuer is not known. This is the case if the issuer is not included in the trusted certificate list.

 > X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT
 



> X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN

> X509_V_ERR_CERT_CHAIN_TOO_LONG

fx X509_V_ERR_CERT_REJECTED

	A	B	C	
6	OpenSSL	GnuTLS	Botan	mbedTLS
7	X509_V_OK		OK	
8	X509_V_ERR_UNSPECIFIED			
9	X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT			
10	X509_V_ERR_UNABLE_TO_GET_CRL		NO_REVOCATION_DATA	
11	X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE			
12	X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE			
13	X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY			
14	X509_V_ERR_CERT_SIGNATURE_FAILURE	GNUTLS_CERT_SIGNATURE_FAILURE	SIGNATURE_ERROR	MBEDTLS_
15	X509_V_ERR_CRL_SIGNATURE_FAILURE	GNUTLS_CERT_SIGNATURE_FAILURE	CRL_BAD_SIGNATURE	
16	X509_V_ERR_CERT_NOT_YET_VALID	GNUTLS_CERT_NOT_ACTIVATED	CERT_NOT_YET_VALID	MBEDTLS_
17	X509_V_ERR_CERT_HAS_EXPIRED	GNUTLS_CERT_EXPIRED	CERT_HAS_EXPIRED	MBEDTLS_
18	X509_V_ERR_CRL_NOT_YET_VALID	GNUTLS_CERT_REVOCATION_DATA_ISSUED_IN_FUTURE	CRL_NOT_YET_VALID	MBEDTLS_
19	X509_V_ERR_CRL_HAS_EXPIRED	GNUTLS_CERT_REVOCATION_DATA_SUPERSEDED	CRL_HAS_EXPIRED	MBEDTLS_
20	X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD			MBEDTLS_
21	X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD			MBEDTLS_
22	X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD			
23	X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD			
24	X509_V_ERR_OUT_OF_MEM			
25	X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT	GNUTLS_CERT_SIGNER_NOT_FOUND	CANNOT_ESTABLISH_TRUST	
26	X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN	GNUTLS_CERT_SIGNER_NOT_FOUND		
27	X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY	GNUTLS_CERT_SIGNER_NOT_FOUND	CERT_ISSUER_NOT_FOUND	
28	X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE			
29	X509_V_ERR_CERT_CHAIN_TOO_LONG			
30	X509_V_ERR_CERT_REVOKED	GNUTLS_CERT_REVOKED		
31	X509_V_ERR_INVALID_CA	GNUTLS_CERT_SIGNER_NOT_CA		
32	X509_V_ERR_PATH_LENGTH_EXCEEDED	GNUTLS_CERT_SIGNER_CONSTRAINTS_FAILURE		
33	X509_V_ERR_INVALID_PURPOSE	GNUTLS_CERT_PURPOSE_MISMATCH		
34	X509_V_ERR_CERT_UNTRUSTED			
35	X509_V_ERR_CERT_REJECTED			


x509errors.org

Summary of our work

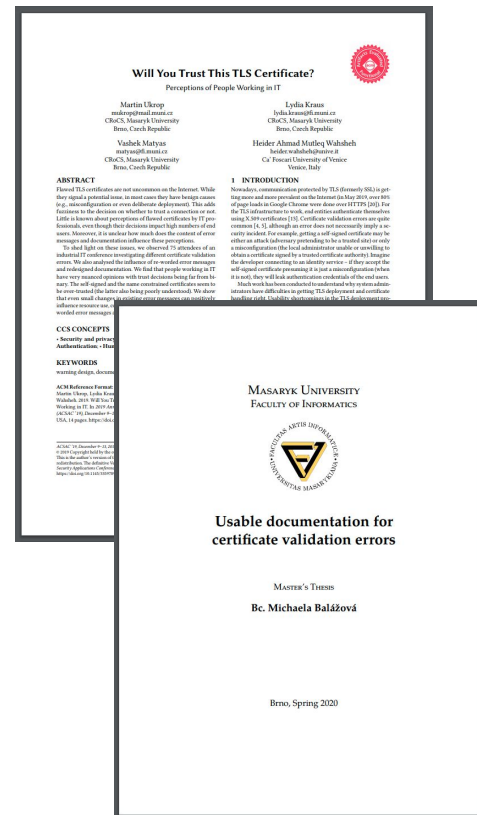
1. Empirical experiments with IT professionals asking for their opinions and preferences
(attendees of **DEVCONF**.cz 2017, 2018, 2020)
2. Project Usable X.509 errors consolidating and improving existing documentation.



x509errors.org

Experience exchange

- Read our research papers (email me if interested in the current, for the past papers check crocs.fi.muni.cz/publications/keywords/usablesec)
- Help us improve the new documentation draft (we are not tech writers, we may miss “basic” things)



May your documentation always be usable!

(And lead to secure code!)



Interested?

Check out the project at <https://x509errors.org>

Write me to mukrop@mail.muni.cz

CRCS

Centre for Research on
Cryptography and Security

Martin Ukrop

Masaryk University, Czech Republic

Ph.D. research cooperation with Red Hat Czech

