Masaryk University
Faculty of Informatics

Usable documentation for certificate validation errors

Master's Thesis

Bc. Michaela Balážová

Brno, Spring 2020

This is where a copy of the official signed thesis assignment and a copy of the Statement of an Author is located in the printed version of the document.

Declaration

Hereby I declare that this paper is my original authorial work, which I have worked out on my own. All sources, references, and literature used or excerpted during elaboration of this work are properly cited and listed in complete reference to the due source.

Bc. Michaela Balážová

Advisor: RNDr. Martin Ukrop

Acknowledgements

I would like to thank my advisor RNDr. Martin Ukrop for his guidance, help, friendly approach, and valuable advice during the whole process of the thesis creation.

I thank Martin, Palo, and Lydia for the help at DevConf, and all the respondents for the participation.

I also want to thank my parents for their support not only during my studies but throughout my life. (Ďakujem Vám, rodičia moji milí, za Vašu lásku a podporu.)

Thanks also go to the professors and teachers for their work and effort to prepare us for professional life.

Abstract

This thesis proposes new documentation for three chosen certificate validation errors. The evaluation of the new documentation, as well as comparison with the current documentation, was done via surveys performed on IT professionals during an international open-source conference.

Keywords

X.509 certificates, usability, documentation, validation errors, survey

Contents

1 Introduction

Secure communication via the Internet is nowadays considered as a basic requirement. One of the possibilities to achieve this is to use public-key cryptography, which uses public-key certificates. Every time, when a certificate is being used, its trust has to be evaluated. When something goes wrong, an error has to be shown. There are plenty of kinds of errors, which can occur. Some of them are quite frequent, while others are occasional. In any case, developers have to know how to handle the error and what they are supposed to do. To help developers to understand an error, there is documentation, which should accompany developers.

Currently, there are more libraries available that offer trust evaluation of certificates. Each library has implemented its own set of possible errors, together with its own documentation. But none of the most used libraries has complete documentation describing the cause of the error and other useful information for developers to handle the error. Thus, there is a project called Usable X.509 errors[1], which aims to improve the documentation problem, and this thesis is part of the project.

However, to write useful documentation for certificate validation errors aimed at developers, the research had to be conducted to find out what do the developers expect from the documentation – what should be included in the documentation, what they currently miss, what they do not like about the documentation, how long should it be. Also, whether the majority is in accordance with the requirements or whether it is a personal preference.

To answer these questions, a research was conducted during the international open-source conference DevConf hold in Brno, Czech Republic, in January 2020. Each participant evaluated two types of documentation for a certificate error. The first documentation was adopted from the OpenSSL library, the second one was newly proposed with intention to provide better documentation, to let the participants compare both documentations and to find out what they like and do not like about the documentation and how to improve the documentation further.

1. `https://x509errors.org/`

The structure of the thesis is as follows: Chapter 2 introduces public-key certificates. Chapter 3 analyzes the current state of the documentation for certificate validation errors of the most used libraries, related work in the writing documentation, and motivation for the thesis. Chapter 4 describes the preparation before the conference and research settings. Chapter 5 brings the results of the survey. Chapter 6 summarizes the recommendations for writing the documentation, and, finally, Chapter 7 concludes the thesis.

2 Public-key certificates

Public-key certificates are used in public-key cryptography. In the public-key cryptography, each entity possesses a pair of keys – a private key and a public key. The private key has to be kept secret, whereas the public key is designated to be published publicly [1]. These two keys are associated, and there is a need to prove that an entity possesses both associated keys. Such a binding is provided by a public-key certificate, which is issued and signed by Certificate Authority (CA), which has the role of the trusted anchor [2].

The next section describes X.509 certificates together with their structure. Then, X.509 extensions are explained, and, finally, the process of validation of X.509 certificates is characterized.

2.1 X.509 certificates

An X.509 certificate is a certificate, which adheres to X.509 format, the official standard for public-key certificates. X.509 standard has three versions; the current one is version 3, marked as X.509v3 [3]. X.509 certificates are data structures that link the values of the public keys to the associated entities [4]. The X.509 certificates prevent man-in-the-middle attacks and ensure the integrity and authenticity of public keys [5, 6].

X.509 certificates are used in many applications and many Internet protocols. They are widely used in SSL/TLS (Secure Sockets Layer/ Transport Layer Security) protocols to allow secure access to web sites and S/MIME (Secure/Multipurpose Internet Mail Extensions) and PEM (Privacy Enhanced Mail) protocols to secure e-mails. Other technologies relying on X.509 certificates include IPsec (Internet Protocol Security), user authentication, e-commerce protocols, such as SET (Secure Electronic Transaction), software updates in modern operating systems, or various code-signing schemes, for example, Java Archives or Microsoft Authenticode [7, 8, 4].

X.509 certificates have a hierarchical structure instead of a flat structure [3]. At the top-level, each X.509v3 certificate contains three fields [4]:

- *tbsCertificate* – carries information about the subject and the issuer of the certificate, contains public key associated with the subject, validity period of the certificate, and other information associated with the certificate. The structure of the field is described below.

- *signatureAlgorithm* – identifier of the algorithm used by the CA to sign the certificate.

- *signatureValue* – a value of the digital signature for the *tbsCertificate* field. By this value, the CA confirms the correctness of the information provided in the *tbsCertificate* field, including the correct binding between the public key's information and the subject of the certificate.

tbsCertificate field of X.509v3 is structured at the top-level as follows:

- *version* – specifies the version of the certificate. The default value is 0 for version 1. The other possibilities are value 1 for version 2, and value 2 for version 3.

- *serialNumber* – a unique integer value within issuing CA; *issuer* and *serialNumber* can be used to identify the certificate unambiguously.

- *signature* – identifier of the algorithm used by CA to sign the certificate.

- *issuer* – identifies the entity that issued and signed the certificate; it can be specified by attributes such as country, organization, common name, and others.

- *validity* – determines the time frame when the certificate is valid and during which the CA maintains information about the certificate. It is compound from two fields – *notBefore* (determines the beginning of the validity of the certificate) and *notAfter* (determines the end of the validity of the certificate).

- *subject* – identifies the entity that holds a private key associated with the public key stored in the *subjectPublicKeyInfo* field. It can be specified by the same attributes as the *issuer* field. The

subject can be specified either in the *subject* field, or in the *subjectAltName* extension field, or at both places.

- *subjectPublicKeyInfo* – contains public key together with the identification of an algorithm for which the public key is meant to be used.
- *issuerUniqueID* – bit string uniquely identifying issuing CA in case the issuer name would be reused over time. This field is optional and can be used only with version 2 or version 3. It is recommended not to use this field and not to reuse issuer names for different entities [4].
- *subjectUniqueID* – bit string uniquely identifying the subject in case the subject name would be reused over time. This field is optional and can be used only with X.509 version 2 or version 3. It is recommended not to use this field and not to reuse subject names for different entities [4].
- *extensions* – contains a set of one or more certificate extensions, which are characterized in the next section. The field is optional and can be used only with the X.509 version 3 [3, 2, 9, 4].

2.2 X.509 extensions

The *extensions* field contains one or more certificate extensions, which hold additional information about users or public keys or express possible relationships between CAs. Each extension consists of up to three fields [4]:

- *extnID* – unique identifier of the extension.
- *critical* – boolean value determining whether the extension is critical or not. The default value is false.
- *extnValue* – the data to be processed; the data depends on the extension type.

The extension marked as critical must be processed. If the party verifying the certificate cannot recognize the extension marked as critical, or critical extension contains information that is not recognized or

cannot be processed, the party must reject the certificate. An extension marked as non-critical must be processed if it is recognized, but it may be ignored if it is not recognized.

There are many standardized extensions; however, it is possible to implement also private extensions. Some of the more important standardized extensions are:

- *Subject alternative name* – it can be used to replace the *subject* field, or to provide additional identifiers for the subject bounded to the certificate. The additional identifiers can include an e-mail address, a DNS (Domain Name System) name, an IP (Internet Protocol) address, a URI (Uniform Resource Identifier), or others. If multiple identifiers or multiple instances of an identifier are provided, the subject field is not sufficient, and the subject alternative name extension has to be used.

- *Key usage* – determines the purposes for which the key contained in the certificate can be used. For example, key usage extension can restrict the usage of an RSA public key only to encryption, which implies restriction of its usage for signature verification.

- *Basic constraints* – signifies whether the subject of the certificate is CA or not. In the case of CA, it further specifies the maximum possible amount of non-self-issued intermediated certificates in a valid certification path, which can follow this certificate [4, 6, 3].

2.3 Validation of X.509 certificates

The primary purpose of validation of X.509 certificates is to verify the binding between the subject of the certificate and the subject's public key. The verification is based on the public key of a trusted anchor, which is usually top-level CA [4]. The simplified description of the X.509 certificate validation, focused on describing the typical validation steps, follows [10]:

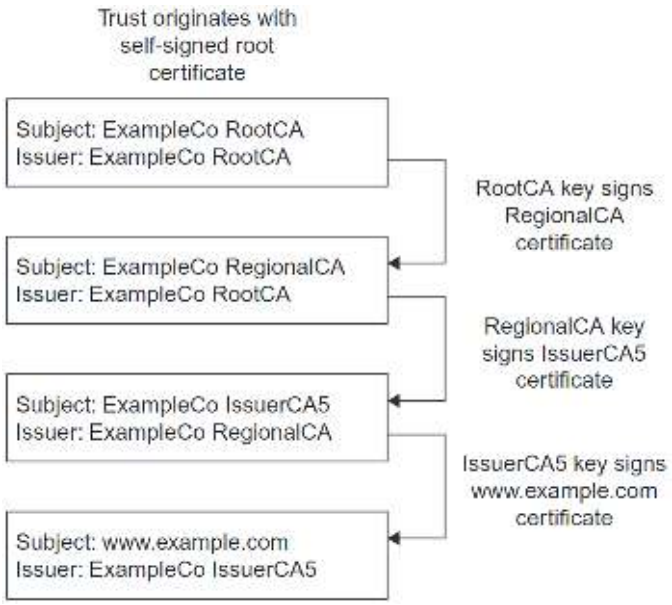

Figure 2.1: Certificate chain [10]

1. Chain construction and signature validation

   Firstly, the signature of the target certificate has to be validated in order to trust the content of the certificate. To check the signature, we need the certificate of CA, which issued the target certificate. Essentially, it has to hold that the issuer field of the target certificate is the same as the subject field of the CA certificate. When we obtain the CA certificate, the target certificate signature is checked using the public key of the CA certificate. If this CA is not a trusted anchor, the validation chain continues. The CA certificate becomes the target certificate, which needs to be validated. The validation chain stops when the trusted anchor is reached. The concept of a certificate chain is shown in Figure 2.1, a real-world example of displaying a certification path in the Google Chrome browser is shown in Figure 2.2.

2. Certificate fields' validation

   When a chain, starting with a target certificate and ending with a trusted anchor certificate, is constructed and all the signatures

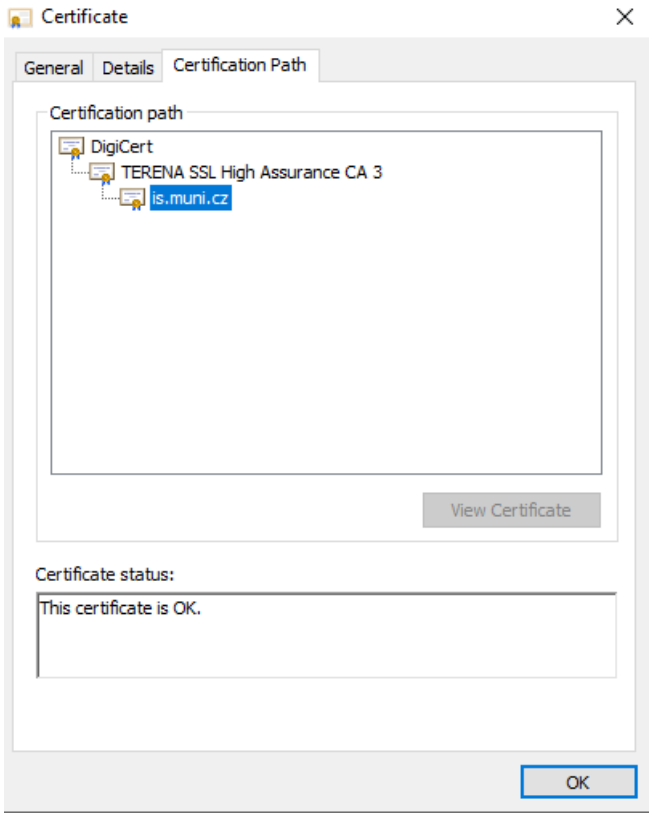

Figure 2.2: Certification path for is.muni.cz displayed in the Google Chrome browser

are validated, some of the field values in the certificates have to be also checked. The first one to be checked is the validity field, to ensure the certificate chain times are correct. Then, for X.509v3, the extensions field has to be checked. There are many kinds of restrictive extensions that have to hold, for example, key usage or basic constraints extensions explained above.

3. Revocation check

   If a certificate contains information which is no longer valid, or private key has been compromised, the certificate has to be revoked [11]. When validating a certificate, the third step is to check whether the certificate was revoked or not to ensure the certificate is still valid. It is performed using either CRL (Certificate Revocation List) or OCSP (Online Certificate Status Protocol) [10].

If all steps of the validation of a certificate succeed, the indication of success should be returned. If anything fails during the verification, an appropriate error should be returned.

3 Related work and motivation

This chapter describes the current state of the documentation for the errors of the most used cryptographic libraries. At the same time, it points to the needed improvements in this scope. Therefore, the project Usable X.509 errors is introduced, which aims to improve the error documentation. Finally, the related work concerning the writing documentation is presented.

3.1 Cryptographic libraries

There are many cryptographic libraries, which offer certificate validation. According to the research done by Nemec et al. [12], the most used cryptographic library for RSA public key generation is the OpenSSL library[1]. As far as I know, there are no studies measuring the usage of cryptographic libraries for certificate validation. The mentioned research brings a valuable overview of the usage of the cryptographic libraries for the RSA public key generation, which could be generalized, with some limitations, and be used for usage estimation of the libraries for certificate validation. Other popular libraries according to the study are Microsoft CryptoAPI[2], Nettle[3] (low-level library, on which GnuTLS library[4] depends [13]), Libgcrypt[5], Mbed TLS[6], Botan[7], wolfSSL[8], OpenJDK[9].

The libraries differ in the granularity of the certificate validation error codes, as well as in the design of the documentation for the errors. The design could be divided into three categories:

1. https://www.openssl.org/
2. https://docs.microsoft.com/en-us/windows/win32/seccrypto/cryptoapi-system-architecture
3. https://www.lysator.liu.se/ nisse/nettle/
4. https://www.gnutls.org/index.html
5. https://www.gnupg.org/software/libgcrypt/index.html
6. https://tls.mbed.org/
7. https://botan.randombit.net/
8. https://www.wolfssl.com/
9. https://openjdk.java.net/

1. Libraries with dedicated web page for the error description (Microsoft CryptoAPI[10], Libgcrypt[11], wolfSSL[12], OpenJDK[13]);

2. Libraries combining CLI (Command Line Interface) or API (Application Programming Interface) description together with error description on the same web page (OpenSSL[14], GnuTLS[15]);

3. Libraries, which offer error codes only in header files or source files (Mbed TLS[16], Botan[17]).

The granularity of the error codes is summarized in Table 3.1, together with the length of the error description. OpenSSL library is mentioned twice in the table because it has a different set of error codes for CLI and API. The biggest amount of possible certificate validation error codes has the wolfSSL library with 137 codes, followed by the CLI OpenSSL library with 77 codes. 83.3% of all error codes have a single line[18] description. The longest description for an error code has 8 lines from the Microsoft CryptoAPI library. It is common that error description is the same as error code, or very similar to it.

---

10. https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/ns-wincrypt-cert_chain_policy_status, https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/ns-wincrypt-cert_revocation_status, https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/ns-wincrypt-cert_trust_status
11. https://www.gnupg.org/documentation/manuals/gcrypt/Error-Codes.html
12. https://www.wolfssl.com/docs/wolfssl-manual/appendix-c/, https://github.com/wolfSSL/wolfssl/blob/master/wolfssl/error-ssl.h
13. https://docs.oracle.com/javase/8/docs/api/java/security/cert/CertPathValidatorException.BasicReason.html
14. https://www.openssl.org/docs/man1.1.1/man1/openssl-verify.html, https://www.openssl.org/docs/man1.1.1/man3/X509_STORE_CTX_get_error.html
15. https://www.gnutls.org/manual/gnutls.html#gnutls_005fcertificate_005fstatus_005ft
16. https://github.com/ARMmbed/mbedtls/blob/master/library/x509_crt.c
17. https://botan.randombit.net/doxygen/cert__status_8cpp_source.html
18. Definition of the line for our purposes: A4 format with 2.5 cm margins, font Times New Roman, size 12.

Library	1 line	2 lines	3 lines	4+ lines	Total
wolfSSL	137	0	0	0	137
OpenSSL - CLI	66	10	1	0	77
Microsoft CryptoAPI	35	25	4	3	67
Botan	53	0	0	0	53
OpenSSL - API	25	12	5	2	44
Libgcrypt	19	3	4	2	28
Mbed TLS	20	0	0	0	20
GnuTLS	13	2	2	0	17
OpenJDK	7	0	0	0	7
	83.3%	11.6%	3.6%	1.6%	100%

Table 3.1: Amount of error codes and their description length in various cryptographic libraries

It can be demonstrated by an example from the CLI OpenSSL library[19]:

X509_V_ERR_NO_EXPLICIT_POLICY

No explicit policy.

In this case, the documentation does not provide any added value. Therefore there is a project called Usable X.509 errors, which aims to improve the documentation for the certificate validation errors. A more detailed description of the project is in the next section.

3.2 Project Usable X.509 errors

Project Usable X.509 errors [14] arose at the Centre for Research on Cryptography and Security (CRoCS) at Masaryk University. The main goals of the project are:

- creating a taxonomy for certificate validation errors;

19. `https://www.openssl.org/docs/man1.1.1/man1/openssl-verify.html`

- creating proper, understandable documentation for every error, aiming at developers and people working with X.509 certificates;
- creating a web page with the taxonomy and documented errors;
- major cryptographic libraries using the created taxonomy and using or linking the web page with the documentation.

This thesis aims to help with creating the documentation by finding the proper format of the documentation, which is accepted and perceived positively by the majority of developers and concerned people.

3.3 Guidelines for writing documentation

The specific guidelines for writing documentation about errors, aimed at developers, are rare. However, Ukrop et al. [15] investigated the impact of redesigned documentation of X.509 certificate errors. The redesigned documentation helped the IT professionals, on whom the study was conducted, to better understand the errors, and they were able to assess the trust in the certificates better.

Uddin and Robillard [16] concerned with API (Application Programming Interface) documentation. Based on the survey sent to the IT professionals, they made a list of ten types of common problems in the API documentation. The problems were divided into two categories – content and presentation. According to the study, the respondents cared most about the quality content.

There are many more studies concerning the perception of the warnings by the end users [17, 18, 19].

There are also recommendations for writing documentation in general, for composing software documentation, for creating security warnings and dialogues for users. All of these sources can provide some useful advice for writing documentation for errors. Summary of the recommendations, applicable for creating the error documentation, follows:

1. According to the guidelines for writing warnings for computer users [20, 21, 22], it is needed to describe the risk, the conse-

quences of not complying, as well as provide the steps how to avoid the risk.

2. The most crucial part is the explanation of the warnings – explanation of the decision, which a user needs to do, as well as providing all available and needed information to empower them to make the right decision. It includes an explanation of the source of the decision, steps, which can a user follow to make a good decision, pointing out at the unique knowledge, which has a user and which needs to be taken into account when making a decision, and finally, stating possible options with consequent impacts, together with a recommendation of the safest option [23].

3. The warnings have to be also brief and accurate. Otherwise, the purpose of the warning is lost, because more people read shorter text [20, 21, 24].

4. It is needed to attract the attention by a signal, boldly printed word in a warning [22, 24].

5. It is essential to use an organized structure, such as outlined, bulleted, or numerical format. Such warnings are more effective and can maintain attention longer than other formats [22, 24].

6. Application of the well-known, frequently used terms, instead of technical jargon, increases the chance the target audience understands the message [24, 21].

7. It is better to provide specific information rather than general [24].

8. Linguistic properties also play an important role in the warnings. It is recommended to use short sentences. Do not use sophisticated grammatical constructs, for example, conjunctions, which prolong the sentences or grammatical tenses, which complicate the understanding of the messages [25].

4 Research settings

The research aims to find out how do the developers and other IT professionals perceive the current documentation for the certificate validation errors and offer them improved documentation and get feedback for it.

The survey took place during the DevConf conference held in January 2020 in Brno, the Czech Republic, for three days. DevConf is an open-source community conference for developers, testers, admins, and other contributors to open source technologies. It is an annual conference sponsored by Red Hat Czech. We had there a research booth, and we asked people passing by to fill in the questionnaire. They could do it either on our computers or on their own devices when they had time. In the second case, we gave them a link to the questionnaire. We offered them a small reward for participation, which they got after finishing the questionnaire and sharing a secret phrase written at the end of the questionnaire.

This chapter outlines what parts contain the newly proposed documentation, describes the design of the questionnaire, states the research questions, tells about pilot testing and cleaning the data, brings the profile of the survey participants, and explains the process of coding used in qualitative analysis.

4.1 Proposed documentation

The newly proposed documentation for the errors was created based on the recommendations listed in Section 3.3, and also considering the format of redesigned documentation by Ukrop et al. [15]. The proposed documentation for all the three errors can be found in the appendix A.

The newly created documentation consists of several parts:

- The first line represents the error code written in bold capital. Each code starts with 'X509', referring to the X.509 certificates. It continues with 'ERR', pointing on the error, highlighting that there is something wrong. Finally, it ends with the keywords of the problem.

- The second line of the documentation is a description of the problem in one sentence. It is suitable for experienced people who know the background of certificates or their validation, and after reading it, they should know what is going on.
- Four paragraphs follow – Explanation, Security perspective, What to do and Consequences, each describing relevant issues, and at the same time, trying to be as concise as possible.

4.2 Questionnaire design

We created a questionnaire with three main parts. The first part contained existing documentation for a validation error adopted from the OpenSSL library together with the questions related to this documentation. However, the participants did not know that it is OpenSSL documentation in order not to influence them. The second part contained newly proposed documentation for the same error, as was presented in the first part. The wording of the questions, together with the possible options, is listed in the appendix B. The set of questions for the second part was almost the same as in the first part. However, the second part did not ask participants whether they had seen that error before. On the other hand, the second part inquired about the perceived importance of the documentation parts, opinions on removing documentation parts, preferred documentation and reasons for that, and the preferred number of lines for the documentation of the error. Participants also could leave us any related comments. The last part of the questionnaire asked some general questions about education, employment, experience.

The documentation for the errors was shown in this order because the OpenSSL documentation is very brief and does not contain more information than the proposed documentation. Thus it was essential to ask questions about understanding and helpfulness of the documentation first for the OpenSSL documentation and consequently for the proposed documentation, which provided a more detailed explanation.

To find out what problems do the participants see in the documentation, we offered them a list of common documentation flaws based on the survey of Uddin and Robillard [16]. The flaws in the survey are

meant for the API documentation and not all of them were suitable for our survey. Only the relevant types were chosen, together with their description. The description of one of the chosen flaws (incompleteness) did not fit our needs. Therefore we adapt the description to fit the purpose. The list of chosen flaws, used in the questionnaire, with their description follows:

- Incompleteness = Some information is missing in the documentation.
- Ambiguity = The description was mostly complete but unclear.
- Inconsistency = The documentation of elements meant to be combined didn't agree.
- Incorrectness = Some information was incorrect.
- Bloat = The description was verbose or excessively extensive.
- Tangled information = The description was tangled with information the respondent didn't need.

The first four flaws are from the content category, and the remaining two flaws are from the presentation category.

The list of irrelevant and therefore unused flaws in the questionnaire follows:

- Unexplained examples = A code example was insufficiently explained.
- Obsoleteness = The documentation on a topic referred to a previous version of the API.
- Fragmentation = The information related to an element or topic was fragmented or scattered over too many pages or sections.
- Excess structural information = The description of an element contained redundant information about the element's syntax or structure, which could be easily obtained through modern IDEs.

The first two flaws are from the content category, and the remaining two flaws are from the presentation category.

We had three variants of the questionnaire. The question set was the same in all of them, however, they differed in the chosen error for which the documentation was shown. The first error has OpenSSL library code 'X509_V_ERR_CERT_HAS_EXPIRED', further referred to as 'Expired certificate'. The second error has code 'X509_V_ERR_HOSTNAME_MISMATCH', further referred to as 'Hostname mismatch', and the last one is coded as 'X509_V_ERR_UNHANDLED_CRITICAL_EXTENSION' with the reference 'Unhandled critical extension'. The questionnaires with three error variants were distributed randomly.

The selection of the errors and thus also the documentation for the errors used in the questionnaires was based on the OpenSSL library since it is the most used cryptographic library. The errors were chosen considering these criteria: one error, which is common and easy to understand (Expired certificate); another one, which is common but more complicated to understand it from the OpenSSL documentation (Hostname mismatch); and one, which is not common and hard to understand it just from the OpenSSL documentation (Unhandled critical extension).

To take part in the research, participants had to agree with the informed consent and filling in the questionnaire diligently at the beginning of the questionnaire. All the questions in the questionnaire were optional; therefore, the number of responses differs per question.

4.3 Research questions

We defined the following research questions:

1. Which documentation do IT professionals prefer?
2. How long documentation do IT professionals prefer?
3. Does newly proposed longer documentation help IT professionals to understand the problem better?
4. Are IT professionals satisfied with current and proposed documentation?

5. What parts of the documentation are important for IT professionals?

6. What problems can IT professionals see in the documentation?

Moreover, each question asks also whether it differs for different errors and whether it correlates with the previous experience.

4.4 Pilot testing

Before the distribution of the questionnaires at the DevConf conference, we conducted a pilot testing in several rounds. In the first round, three separate questionnaires were originated, each for one error. All closed-ended and one open-ended questions were mandatory, the rest of the open-ended questions were optional. One to two people answered each questionnaire and gave short feedback. In the second round, there was only one questionnaire with a random distribution of the errors. Only one open-ended question was mandatory; all the other questions were optional. Eight people responded to it, and three of them provided detailed feedback. Improvements based on the feedback were included in the last third testing round with the same settings as in the previous round. The questionnaire was sent to 94 students from the Faculty of Informatics, Masaryk University. 3 of them partially and 12 of them fully filled in the questionnaire. No additional feedback was provided, but we could see whether the answers are appropriate, and thus whether the formulation of the questions is proper and the results are usable.

During all three rounds, one open-ended question was mandatory, because we aimed to change the question to multiple choice. To perform it, we needed to collect as many different answers and opinions as possible until the responses begin to repeat. However, we were not able to get enough answers for summarizing them into options. Thus the question stayed open-ended in the final questionnaire.

4.5 Cleaning the data

The questionnaire was created via the LimeSurvey[1] tool. The responses were exported into statistical software IBM SPSS Statistics[2], where they were cleaned and processed. Cleaning of the data was done in several steps. Firstly, we removed all answers where the participants did not agree with the informed consent or with filling in the questionnaire diligently. Secondly, responses with no answer were deleted, since all the questions were optional. In the next step, we checked whether all the values are appropriate – the choice questions had to contain only values listed in the options, the questions with numerical answers had to be from a meaningful interval, and a multiple-choice question, asking whether they would remove a part/some parts from documentation, could not have answered 'yes' (followed by a concrete part) and 'no' at the same time. In this step, three values were canceled in the question asking how many lines of documentation would they prefer. Two of them were extremely large – 4558 and 1337, and the third one was a negative number -1. Also, one value in the multiple-choice question had to be deleted because of checking 'yes' and 'no' answers simultaneously. Subsequently, following the best practices, all missing values were coded into a negative number. Moreover, during the questionnaire creation, one question with the ordinal scale had reversed scale direction, so we had to reverse it back. Finally, we had to set the appropriate scales for the variables by changing the nominal scale to ordinal for questions with Likert scale answers.

4.6 Participants

In the beginning, we had 220 responses. During the cleaning, 30 of them were removed, and the analysis was done with the remaining 190 answers. All the questions were optional, and thus the statistics about the participant are not complete.

Participants in the survey comprised 86.2% (156) of men, 11.6% (21) of women, and 2.2% (4) of people, who determine themselves as another gender (out of 181 respondents). 14.8% (27) are currently stu-

1. https://www.limesurvey.org/
2. https://www.ibm.com/products/spss-statistics

dents of an IT-related discipline (out of 182). Most of the participants (44.8%, 81 persons) reached a master's degree in IT-related discipline, 29.8% (54) bachelor degree, 1.7% (3) postgraduate degree, and the rest (23.8%, 43 persons) does not have a formal education in IT (out of 181).

Almost half of the respondents (48.9%, 89) work as a developer or a software engineer, 7.7% (14) is employed as a tester or a quality assurance engineer, and the third most numerous category is manager position (7.1%, 13), out of 182 respondents.

On average, respondents are employed in an IT-related field for 9.69 ± 7.03 years (median 8), the minimum is 0 years, and the maximum is 35 years.

Most of the participants were from the Czech Republic (31.9%, 58), followed by Polish participants (15.9%, 29) and Indians (10.4%, 19), out of 182. To demonstrate the internationality of the conference, as well as internationality of the participants, who expressed their opinions on the documentation, since the documentation is used worldwide, the list of countries of the respondents, ordered descending according to the number of participants, follows: Czech Republic, Poland, India, Austria, USA, Russia, Germany, Slovakia, Italy, Ireland, Spain, Ukraine, Albania, Croatia, France, Hungary, Netherlands, Brazil, Norway, Slovenia, Belgium, China, Estonia, Japan.

The self-reported knowledge of general computer security was 'good' on average (mean 2.81 ± 0.90, median 3), the knowledge of X.509 certificates was 'fair' on average (mean 3.69 ± 1.06, median 4). We used a Likert scale with the following levels: 'excellent' (coded as number 1), 'very good'(2), 'good' (3), 'fair' (4), 'poor' (5).

Almost two-thirds had used OpenSSL library more than 5 times (62.6%, 114), one-fifth (23.6%, 43) two to five times, 7.7% (14) only once and 6.0% (11) had never used OpenSSL library (out of 182).

4.7 Process of coding

Analysis of qualitative data gained from open-ended questions (see Chapter 5 for explanation) includes the process of coding. Coding means assigning labels to data based on the meaning, the content of data. I used inductive [26] technique for creations of codes – the codes

were not known before the process of coding, but they were emerging gradually while going through all the answers.

5 Results

This chapter presents the answers to the research questions introduced in the previous chapter and some additional comments on the documentation from the respondents. The results come from quantitative and qualitative analysis. Quantitative analysis is based on the closed-ended questions (questions with options), whereas qualitative analysis is based on the open-ended questions (questions without options, the questions require answers in the own words of the respondents). The open-ended questions were used to get participants' opinions on the flaws in the documentation, preferred type of documentation, and other additional comments. The possibility to express their opinions on the flaw had only those who checked 'Yes' or 'Rather yes' for the question asking about the occurrence of the flaw in the documentation, but not all of them wrote their reasoning.

5.1 Which documentation do IT professionals prefer?

The majority of people (157 respondents, 88.7%) prefer the second documentation – the newly proposed one. The first documentation is slightly more preferred for the Expired certificate error. It is probably caused by the fact that this error is widely known and easy to understand. The complete results are shown in Table 5.1

According to a Fisher's exact test, there is not a statistically significant difference in the preferred documentation between participants of different gender ($p = 1.000$), students and non-students ($p = 0.514$), highest reached degree ($p = 0.613$), job position ($p = 0.119$), country ($p = 0.334$), security knowledge ($p = 0.082$), number of times they used OpenSSL library before ($p = 0.707$). However, there was found an association between preferred documentation and X.509 certificate knowledge (Fisher's exact test, $p = 0.008$), Cramer's $V = 0.30$, $p = 0.007$.

The main reasons why respondents prefer the first documentation are short, concise description (9 respondents), clear description (5 respondents), and that it is easy to understand and follow the description (4 respondents).

	First doc		Second doc	
Error	Respondents	%	Respondents	%
Expired certificate	11	18%	49	82%
Hostname mismatch	4	7%	54	93%
Unhandled critical extension	5	9%	54	92%
Total	20	11%	157	89%

Table 5.1: Preferred documentation with and without respect to the error type

Emphasized reasons for preferring the second documentation are explanation how to fix the problem (33 respondents, code WhatToDo in Table 5.2), provision of more details (26 respondents, code MoreDetails), well explained error(24 respondents, code ClearExplanation). The other major reasons are summarized in Table 5.2, together with the number of answers and representative quotes.

5.2 How long documentation do IT professionals prefer?

The minimal preferred number of lines for the documentation is one, and the maximal is 100. The respondents prefer 21.52 ± 12.93 lines on average. A Kruskal-Wallis H test showed that the differences across the errors are not statistically significant ($\chi^2(2) = 2.63, p = 0.27$). Slight distinctions can have two reasons:

1. How known is the error and how difficult is it to understand it.

2. The length of the documentation, which was shown to the participants. It is because the question asking about the preferred number of lines also contained information, how many lines

Code	Code description	Total	Expired certificate	Hostname mismatch	Unhandled crit. extension	Representative quote
WhatToDo	It explains what to do, how to fix the problem.	33	13	8	12	"[...] describes a way how to fix an issue" (Error 2)
MoreDetails	It provides more details.	26	7	13	6	"More information and intuitive." (Error 3)
ClearExplanation	It is clear and well explained.	24	9	9	6	"It provides a more clear overview of the problem [...]" (Error 1)
CompleteInfo	It provides complete/all required information.	24	9	9	6	"All in one place." (Error 2)
RootCause	It explains the root cause, what caused the error, what is wrong.	18	6	5	7	"It says what happened in way I understand it [...]" (Error 1)
NoOtherSources	There is no need to use Google or other sources of information.	15	2	7	6	"I don't have to use another books, google, etc" (Error 3)
Consequences	It contains consequences part.	12	6	2	4	"It shows me causes, consequences, dependencies." (Error 1)
GoodForBeginners	It is helpful for non-experienced users.	12	6	4	2	"Is more helpful to newbies." (Error 1)
Context	It gives context to the error.	11	2	4	5	"I like to have deeper understanding of the problem." (Error 3)

Table 5.2: Reasons for preferring the second documentation. Total, Expired certificate, Hostname mismatch, and Unhandled critical extension columns contain the number of respondents who expressed a similar opinion as is stated in the Code description column. 157 respondents prefer the second documentation, and 137 of them also wrote a comment.

have the second documentation. The Expired certificate error has 27 lines, while the other two errors have 23 lines.

The mode for Expired certificate and Hostname mismatch is the same as the number of lines of documentation, which was shown to them. For Expired certificate, 17 out of 50 respondents prefer 27 lines; for Hostname mismatch, 13 out of 50 respondents prefer 23 lines. The mode for Unhandled critical extension is 20, which is rounded number 23, the number of lines of the shown documentation. It is preferred by 13 respondents out of 52. It implicates that the length of the documentation was accurate for them. The complete statistics are comprised in Table 5.3.

	Expired certificate	Hostname mismatch	Unhandled critical extension	Total
Mean	22.12	19.64	22.75	21.52
Standard deviation	15.39	8.54	13.85	12.93
Minimum	1	2	2	1
First quartile	10.0	15.0	15.3	15.0
Median	25.0	20.0	20.0	20.0
Third quartile	27.0	23.0	24.5	25.0
Maximum	100	50	100	100
Mode	27	23	20	20
Number of lines of the new documentation	27	23	23	-

Table 5.3: Descriptive statistics for the preferred length of the documentation, with and without respect to the error type, expressed in the lines

According to the Kruskal-Wallis H test, there are no significant differences in the preferred length of the documentation between participants of different gender ($\chi^2(2) = 2.50, p = 0.29$), highest reached de-

gree ($\chi^2(3) = 1.70, p = 0.64$), job position ($\chi^2(12) = 5.98, p = 0.98$), country ($\chi^2(23) = 27.69, p = 0.23$), security knowledge ($\chi^2(4) = 4.55$, $p = 0.34$), X.509 certificate knowledge ($\chi^2(4) = 5.90, p = 0.21$), number of times they used OpenSSL library before ($\chi^2(3) = 4.26, p = 0.24$). Mann-Whitney U Test showed no significant differences in the preferred length of the documentation between students and non-students (U = 1269, p = 0.57).

5.3 Does newly proposed longer documentation help IT professionals to understand the problem better?

Overall, 72.1% of respondents (137 out of 190) claimed they understood or rather understood the error after reading the first documentation, whereas after reading the second documentation, 97.8% of respondents (178 out of 182) claimed they understood or rather understood the error. Noticeable was also a difference when they were sure they understood the error, 34.7% (66 out of 190) for the first documentation versus 88.5% (161 out of 182) for the second documentation. The results are displayed in Figure 5.1.

A Wilcoxon signed-rank test showed that there was a statistically significant change in the understanding of the errors after reading the first and the second documentation (N = 182, Z = -9.033, p < 0.001). 110 participants (60.4%) understood the error better after reading the second documentation; 69 people (37.9%) understood it the same, and 3 respondents (1.6%) had worse understanding of the error after reading the second documentation. Understanding was based on self-evaluation.

Regarding the understanding of the individual errors, A Kruskal-Wallis H test showed that after reading the first documentation, there was a statistically significant difference in the understanding between the different errors ($\chi^2(2) = 65.21, p < 0.001$). Expired certificate error and Hostname mismatch error were statistically significantly more understood than Unhandled critical extension error. Expired certificate error was understood by 56% of the participants (37 out

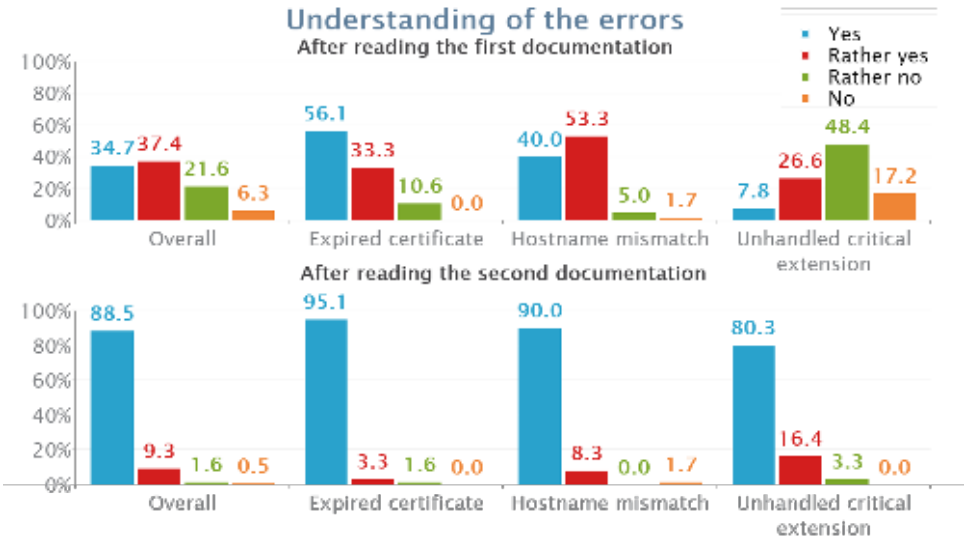

Figure 5.1: Understanding of the errors for the first and the second documentation with and without respect to the individual errors

of 66), Hostname mismatch by 40% (24 out of 60), and Unhandled critical extension by 8% (5 out of 64).

Also after reading the second documentation, a Kruskal-Wallis H test showed a statistically significant difference in the understanding between some of the errors ($\chi^2(2) = 6.53, p = 0.04$), concretely between Expired certificate and Unhandled critical extension errors. The understanding was 95% (58 out of 61) for Expired certificate, 90% (54 out of 60) for Hostname mismatch, and 80% (49 out of 61) for Unhandled critical extension.

A Wilcoxon signed-rank test showed that there was a statistically significant change in the understanding of the errors after reading the first and the second documentation for all three types of the errors (Z = -4.170, p < 0.001 for Expired certificate; Z = -4.988, p < 0.001 for Hostname mismatch; Z = -6.479, p < 0.001 for Unhandled critical extension).

According to the Kruskal-Wallis H test, there are no significant differences in the understanding of the first documentation between participants of different gender ($\chi^2(2) = 4.52, p = 0.10$), highest reached degree ($\chi^2(3) = 5.88, p = 0.12$), job position ($\chi^2(12) = 24.22, p =$

0.02) – no significant differences between groups after applying Bonferroni corrections, country ($\chi^2(23) = 31.41, p = 0.11$), security knowledge ($\chi^2(4) = 14.03, p = 0.01$) – no significant differences between groups after applying Bonferroni corrections, number of times they used OpenSSL library before ($\chi^2(3) = 6.58, p = 0.09$). Mann-Whitney U Test showed no significant differences in the understanding of the first documentation between students and non-students (U = 2396, p = 0.20). However, there were statistically significant differences in the understanding of the first documentation among some groups of the participants, who had various X.509 certificate knowledge ($\chi^2(4) = 26.20, p < 0.001$). Participants with very good or good X.509 knowledge had better understanding than those with fair or poor knowledge.

According to the Kruskal-Wallis H test, there are no significant differences in the understanding of the second documentation between participants of different gender ($\chi^2(2) = 0.69, p = 0.71$), job position ($\chi^2(12) = 10.12, p = 0.61$), country ($\chi^2(23) = 28.28, p = 0.21$), security knowledge ($\chi^2(4) = 4.90, p = 0.30$), X.509 certificate knowledge ($\chi^2(4) = 4.48, p = 0.35$), number of times they used OpenSSL library before ($\chi^2(3) = 7.74, p = 0.052$). Mann-Whitney U Test showed no significant differences in the understanding of the second documentation between students and non-students (U = 1919, p = 0.22). However, there were statistically significant differences in the understanding of the second documentation among some groups of the participants with different highest reached degree ($\chi^2(3) = 13.11, p = 0.004$). After applying Bonferroni corrections, people with bachelor or master degree had better understanding than those with postgraduate degree. But it is needed to note that there were only 3 people (1.7%) with postgraduate degree, whereas bachelor degree reached 54 people (28.4%) and master degree 81 people (42.6%).

5.4 Are IT professionals satisfied with current and proposed documentation?

Based on the direct question about satisfaction with the documentation, 23.6% of respondents (45 out of 190) stated that they are ex-

tremely or very satisfied with the first documentation, whereas 84.0% of the respondents (152 out of 181) are extremely or very satisfied with the second documentation. The results are shown in Figure 5.2, in the left chart.

According to a Wilcoxon signed-rank test, the change in satisfaction with the documentation is statistically significant (N = 181, Z = -10.297, $p < 0.001$). 149 respondents (82.3%) are more satisfied with the second documentation; 22 people (12.2%) are equally satisfied with both documentations, and 10 participants (5.5%) are more satisfied with the first documentation.

According to the Kruskal-Wallis H test, there are no significant differences in the satisfaction with the first documentation between participants of different gender ($\chi^2(2) = 0.42, p = 0.81$), highest reached degree ($\chi^2(3) = 3.86, p = 0.28$), job position ($\chi^2(12) = 19.56, p = 0.08$), security knowledge ($\chi^2(4) = 9.48, p = 0.05$), number of times they used OpenSSL library before ($\chi^2(3) = 1.49, p = 0.69$). Mann-Whitney U Test showed no significant differences in the satisfaction with the first documentation between students and non-students (U = 2392, p = 0.22). However, there were statistically significant differences in the satisfaction with the first documentation and participants' countries ($\chi^2(23) = 41.62, p = 0.01$) and X.509 security knowledge ($\chi^2(4) = 13.75, p = 0.01$). After applying Bonferroni corrections, Indians are more satisfied with the first documentation than Czechs, and people with very good or good X.509 certificate knowledge are more satisfied than those with poor knowledge.

According to the Kruskal-Wallis H test, there are no significant differences in the satisfaction with the second documentation between participants of different gender ($\chi^2(2) = 1.90, p = 0.39$), highest reached degree ($\chi^2(3) = 5.58, p = 0.13$), job position ($\chi^2(12) = 11.25, p = 0.51$), country ($\chi^2(23) = 31.12, p = 0.12$), security knowledge ($\chi^2(4) = 5.71, p = 0.22$), number of times they used OpenSSL library before ($\chi^2(3) = 1.47, p = 0.69$). Mann-Whitney U Test showed no significant differences in the satisfaction with the second documentation between students and non-students (U = 1956, p = 0.60). Kruskal-Wallis H test showed differences in the satisfaction with the second documentation between participants with different X.509 certificate knowledge ($\chi^2(4) = 11.90, p = 0.02$). After applying Bonferroni corrections, people with good knowldge of X.509 certificates were more

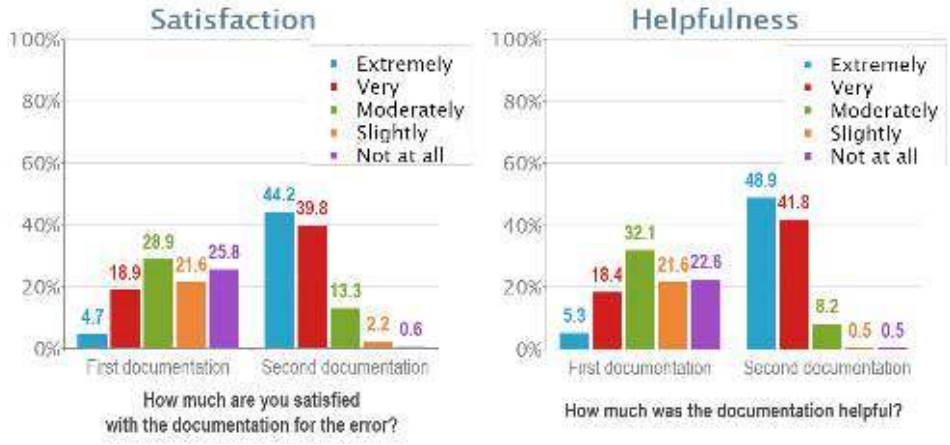

Figure 5.2: Satisfaction with both types of documentation without respect to the types of errors is on the left side; on the right side is the helpfulness of the documentation

satisfied with the second documentation than those with poor knowledge.

Extremely or very satisfied with the first documentation were 47% of respondents (31 out of 66) with the Expired certificate, 20% (12 out of 60) with the Hostname mismatch, and 3% (2 out of 64) with the Unhandled critical extension. For the second documentation, the satisfaction counts 87% (52 out of 60), 77% (46 out of 60), and 89% (54 out of 61), respectively.

A Wilcoxon signed-rank test showed that the change in satisfaction with the documentation is statistically significant also for the individual errors ($Z = -5.059$, $p < 0.001$ for Expired certificate; $Z = -5.772$, $p < 0.001$ for Hostname mismatch; $Z = -6.684$, $p < 0.001$ for Unhandled critical extension).

There is a strong association between satisfaction with the documentation and helpfulness of the documentation: ($\chi^2(4) = 178.72$, $p < 0.001$), Kendall's Tau-b = 0.77, $p < 0.001$ for the first documentation, for the second documentation chi-square test could not be used, therefore Fisher's exact test was used with $p < 0.001$, Kendall's Tau-b = 0.60, $p < 0.001$. The comparison is in Figure 5.2, where can be seen

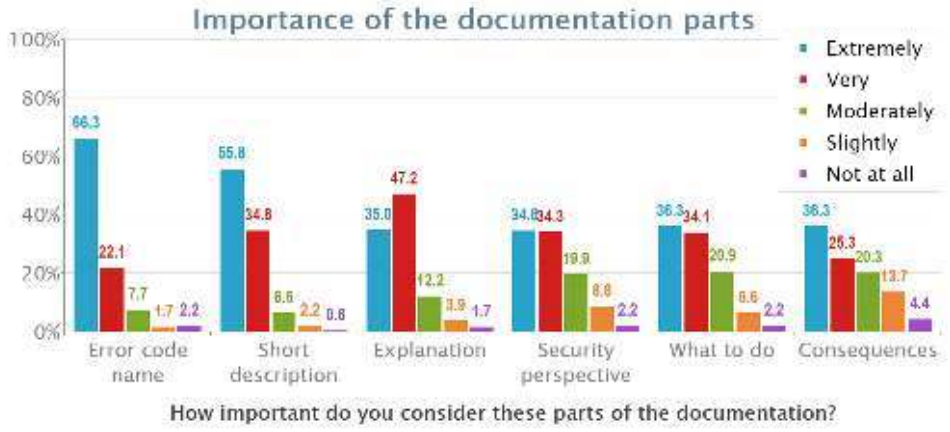

Figure 5.3: Importance of the parts of the second documentation

the similar distribution between satisfaction and helpfulness within the same type of the documentation.

No association was found between satisfaction with the first documentation and the number of used OpenSSL library ($p = 0.46$, Fisher's exact test), as well as between satisfaction with the second documentation and the number of used OpenSSL library ($p = 0.86$, Fisher's exact test).

5.5 What parts of the documentation are important for IT professionals?

For most of the respondents, about two thirds (120 out of 181), the most important is an Error code name, followed by a Short description with more than half of the respondents (101 out of 181). On the other hand, the least important is the Consequences part (4.4%, 8 out of 182). The results are shown in Figure 5.3. Friedman's test showed that there were statistically significant differences in perceived importance between the different documentation parts ($\chi^2(5) = 83.35, p < 0.001$). Statistically significant differences were between Error code name and all other categories, besides Short description, and between Short description and all other categories, except Error code name.

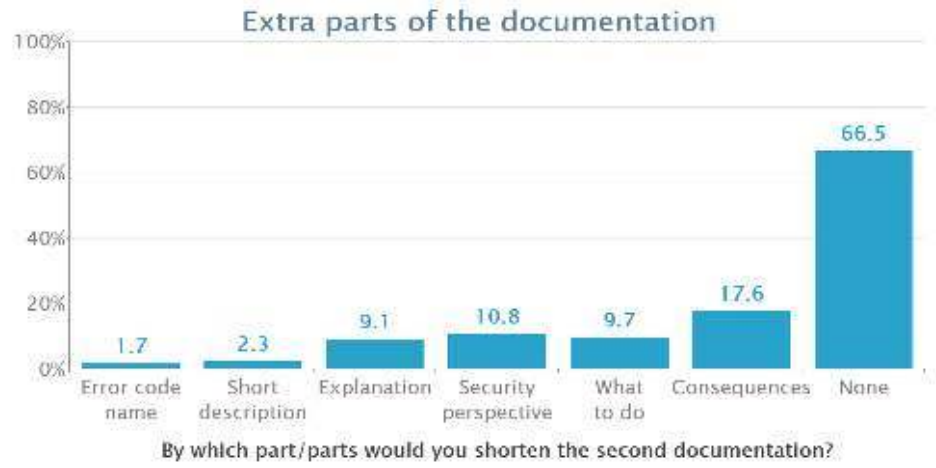

Figure 5.4: The number of respondents who would remove the individual parts from the second documentation; multiple-choice was possible

It is in accordance with what the majority of the respondents stated they would remove. 17.6% (31 out of 176) of the respondents would remove the Consequences part; 10.8% (19 out of 176) would remove the Security perspective part. However, two-thirds of respondents (66.5%, 117 out of 176) would not shorten the second documentation by removing any of its parts. The outcome is in Figure 5.4. Cochran's Q test determined that there was a statistically significant difference in the will to remove some parts of the documentation ($\chi^2(6) = 341.92, p < 0.001$). Statistically significant differences were between removing Consequences part and Error code name and Short description parts, and between not removing any part and all the other categories.

A Kruskal-Wallis H test was conducted to determine if the perceived importance of different parts of the documentation was different for participants with different gender, highest reached degree, job position, country, security knowledge, X.509 certificate knowledge, and used OpenSSL library. To determine differences between students and non-students, Mann-Whitney U Test was executed. Results are served only for statistically significant differences: Explanation part and X.509 certificate knowledge ($\chi^2(4) = 12.31, p = 0.02$) – people with excellent X.509 certificate knowledge consider the Explanation

part more important than those with very good knowledge. Security perspective part and security knowledge ($\chi^2(4) = 9.83, p = 0.04$) – people with excellent security knowledge consider Security perspective part more important than those with good knowledge. Security perspective part and X.509 certificate knowledge ($\chi^2(4) = 10.83, p = 0.03$) – people with good X.509 knowledge regard Security perspective part more important than people with poor knowledge. What to do part and X.509 certificate knowledge ($\chi^2(4) = 11.71, p = 0.02$) – participants with good X.509 certificate knowledge perceive the What to do part more important than people with very good knowledge, and respondents with fair knowledge consider it more important than those with very good knowledge. Consequences part and country ($\chi^2(4) = 10.83, p = 0.03$) – Indians consider Consequences part more important than Czechs.

Regarding the differences in importance for different parts of the documentation between different errors, Kruskal-Wallis H test showed statistically significant differences only for Explanation part ($\chi^2(2) = 6.91, p = 0.03$) and What to do part ($\chi^2(2) = 6.29, p = 0.04$). Both parts were more important for Unhandled critical extension error than for Hostname mismatch error.

5.6 What problems can IT professionals see in the documentation?

Flaws in the first documentation

The most significant flaws of the first documentation are incompleteness and ambiguity. 61.6% (117 out of 190) of the respondents consider it incomplete, 36.9% (70 out of 190) think it is ambiguous. The results are displayed in Figure 5.5. According to a Kruskal-Wallis H test, there is not a statistically significant difference in perceiving flaws among the error types, except perceiving incompleteness ($\chi^2(2) = 57.74, p < 0.001$), where the Expired certificate has 30% (20 out of 66), Hostname mismatch 72% (43 out of 60) and Unhandled critical extension 84% (54 out of 64).

Kruskal-Wallis H test showed that there is not a statistically significant difference in perceiving the first documentation incomplete and

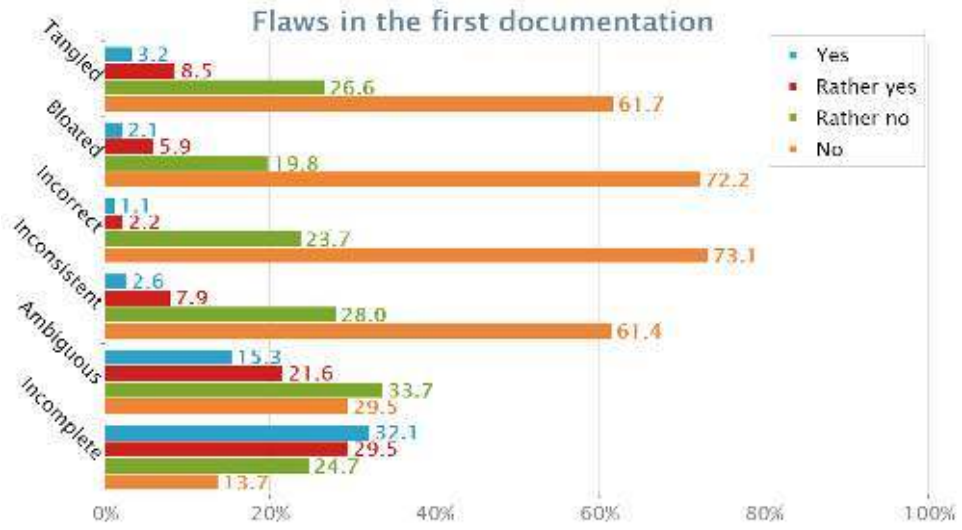

Figure 5.5: Opinions on the flaws in the first documentation

partcicipants' gender ($\chi^2(2) = 2.05, p = 0.36$), highest reached degree ($\chi^2(3) = 4.91, p = 0.18$), job position ($\chi^2(12) = 15.60, p = 0.21$), country ($\chi^2(23) = 27.25, p = 0.25$), X.509 certificate knowledge ($\chi^2(4) = 5.50, p = 0.24$), number of times they used OpenSSL library before ($\chi^2(3) = 0.60, p = 0.90$). Mann-Whitney U Test showed no significant differences in perceiving the first documentation incomplete between students and non-students ($U = 2021$, $p = 0.77$). However, there is a statistically significant difference in perceiving the first documentation incomplete between participants with different security knowledge ($\chi^2(4) = 10.45, p = 0.03$). After applying Bonferroni corrections, people with good security knowledge perceived the first documentation more often incomplete than those with very good security knowledge.

However, there was an association between understanding of error after reading the first documentation and considering the first documentation incomplete ($\chi^2(3) = 28.27 p < 0.001$), Cramer's $V = 0.39$, $p < 0.001$.

Kruskal-Wallis H test showed that there is not a statistically significant difference in perceiving the first documentation ambiguous and partcicipants' gender ($\chi^2(2) = 0.35, p = 0.84$), highest reached de-

gree ($\chi^2(3) = 4.74, p = 0.19$), job position ($\chi^2(12) = 11.37, p = 0.50$), country ($\chi^2(23) = 33.44, p = 0.07$), security knowledge ($\chi^2(4) = 4.17$, $p = 0.38$), X.509 certificate knowledge ($\chi^2(4) = 8.07, p = 0.09$), number of times they used OpenSSL library before ($\chi^2(3) = 1.83, p = 0.61$). Mann-Whitney U Test showed no significant differences in perceiving the first documentation ambiguous between students and non-students (U = 2053, p = 0.87).

Qualitative analysis showed that most of the respondents considered the first documentation to be incomplete because it is too short, and more details are needed (30 respondents, code MissingInfo in Table 5.4). The second largest group complained about missing concrete values (21 respondents, code RealValues), for example, when the certificate expired for the Expired certificate error. However, they did not realize that this is general documentation, so it is not possible to have there real, concrete values based on the concrete circumstances. Nevertheless, it would be possible to add such values in the applications which validate the certificates when an error is shown. Then, the third most numerous group of people would like to know how to fix the problem, what they should do when they receive such an error (19 respondents, code WhatToDo). For the ambiguity problem, the majority of respondents miss the explanation of used terms and field names (13 respondents, code TermExplanation in Table 5.5). Other cases for incompleteness and ambiguity, together with the description, amount of answers, and representative quotes, can be found in Table 5.4 and Table 5.5.

It is worthy of mentioning that some people considered this short documentation bloated or tangled. The reasons for bloated documentation are repeating the same information in the error code and then in the description (2 respondents out of 15), used extra conjunction (1 respondent), and too long error id (1 respondent). The documentation was considered tangled because of repeating the same information (the same reasoning as for bloated documentation; 5 respondents out of 22), 3 respondents wrote that there were too many details. Regarding inconsistency and incorrectness, the written opinions did not reflect the center of the problem.

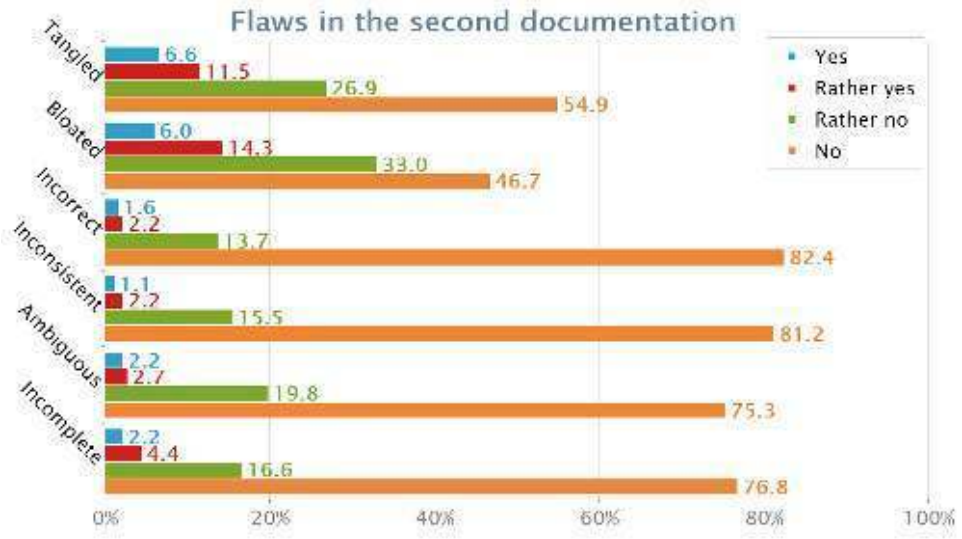

Figure 5.6: Opinions on the flaws in the second documentation

Flaws in the second documentation
The second documentation is often seen as bloated or tangled. 20.3% (37 out of 182) consider it bloated and 18.1% (33 out of 182) tangled. The outcome is shown in Figure 5.6. The differences among the error types are not statistically significant.

Kruskal-Wallis H test showed that there is not a statistically significant difference in perceiving the second documentation bloated and partcicipants' gender ($\chi^2(2) = 0.28, p = 0.87$), highest reached degree ($\chi^2(3) = 1.01, p = 0.80$), job position ($\chi^2(12) = 9.49, p = 0.66$), country ($\chi^2(23) = 30.59, p = 0.13$), X.509 certificate knowledge ($\chi^2(4) = 6.25, p = 0.18$), number of times they used OpenSSL library before ($\chi^2(3) = 2.70, p = 0.44$). Mann-Whitney U Test showed no significant differences in perceiving the second documentation bloated between students and non-students (U = 1645, p = 0.06). However, there is a statistically significant difference in perceiving the second documentation bloated between participants with different security knowledge ($\chi^2(4) = 16.78, p = 0.002$). After applying Bonferroni corrections, people with very good security knowledge perceived the second documentation more often bloated than those with excellent security knowledge.

Code	Code description	Total (117;92)	Expired certificate (20;15)	Hostname mismatch (43;13)	Unhandled crit. extension (54;33)	Representative quote
MissingInfo	Not enough information, too short, needed more details.	30	4	10	16	"the information is not enough" (Error 1)
RealValues	It does not provide concrete values (when the certificate expired, what was not matching, what extension is unhandled)	21	3	11	7	"I believe it will be usefully to see in the error message when the certificate has been expired" (Error 1)
WhatToDo	Misses suggested solution, how to fix the error.	19	3	7	9	"What can I do to fix it? " (Error 3)
NoDocumentation	There is no documentation, no new information, documentation is the same as is the error code.	15	0	6	9	"It doesn't provide any information beyond what the error code itself does" (Error 2)
TermExplanation	Explanation of terms or field names used in the documentation. Explanation whether CN or SAN fields are used.	14	2	5	7	"I have no idea what the extension is and what does it mean that it is not handled." (Error 3)
RootCause	Explanation of the root cause, what caused the error.	14	0	5	9	"I'm missing reason of the mismatch." (Error 2)

Table 5.4: Reasons for the incompleteness in the first documentation. The first number in the heading expresses how many respondents considered the first documentation incomplete or rather incomplete. The second number shows how many of them expressed their opinions on the incompleteness.

Code	Code description	Total (70;52)	Expired certificate (24;19)	Hostname mismatch (21;12)	Unhandled crit. extension (25;21)	Representative quote
TermExplanation	Explanation of terms or field names used in the documentation. Explanation whether CN or SAN fields are used.	13	2	6	5	"Doesn't tell me: why it's unhandled, why it's critical and what's an extension." (Error 3)
RootCause	Explanation of the root cause, what caused the error.	7	0	0	7	"Because I don't know what caused this error" (Error 3)
TimeUnderstanding	Reference to the date and current time is hard to understand.	4	4	0	0	"I had to think some time what the descriptive text means." (Error 1)
ComplicatedWording	Complicated wording, unclear explanation.	4	4	0	0	"wording is complicated, a bit unclear" (Error 1)
NoDocumentation	There is no documentation, nothing relevant, it is too short.	4	0	2	2	"Very hard to find anything relevant" (Error 3)

Table 5.5: Reasons for the ambiguity in the first documentation. The first number in the heading expresses how many respondents considered the first documentation ambiguous or rather ambiguous. The second number shows how many of them expressed their opinions on the ambiguity.

Moreover, no association was found between understanding the error after reading the first documentation and considering the second documentation bloated ($\chi^2(3) = 1.52, p = 0.68$).

Kruskal-Wallis H test showed that there is not a statistically significant difference in perceiving the second documentation tangled and partcicipants' gender ($\chi^2(2) = 1.09, p = 0.58$), highest reached degree ($\chi^2(3) = 0.40, p = 0.94$), job position ($\chi^2(12) = 9.07, p = 0.70$), country ($\chi^2(23) = 27.42, p = 0.24$), X.509 certificate knowledge ($\chi^2(4) = 4.96, p = 0.29$), number of times they used OpenSSL library before ($\chi^2(3) = 0.19, p = 0.98$). Mann-Whitney U Test showed no significant differences in perceiving the second documentation tangled between students and non-students (U = 1846, p = 0.28). However, there is a statistically significant difference in perceiving the second documentation tangled between participants with different security knowledge ($\chi^2(4) = 13.86, p = 0.01$). After applying Bonferroni corrections, people with very good security knowledge perceived the second documentation more often tangled than those with fair security knowledge.

The qualitative analysis revealed that the second documentation is perceived to be bloated mainly because of its length and much information contained in it (16 respondents, code TooLong in Table 5.6). Another more numerous reasoning is that the explanation part is either too long or not needed at all (5 respondents, code ExtraExplanation). For the tangled documentation, the respondents stated that what to do part is not necessary (7 respondents, code ExtraWhatToDo in Table 5.7) and that it contains much information (7 respondents, code MuchInfo). The other reasoning for bloated and tangled documentation, together with the number of answers and representative quotes, can be found in Table 5.6 and Table 5.7. The other flaws of the documentation were stated only by a few of the respondents. They missed the explanation of some terms (incompleteness case, 3 respondents out of 12) and suggested solution (incompleteness case, 2 respondents out of 12). They considered the text to have complicated wording or text construction (ambiguity case, 2 respondents out of 9). One participant noticed outdated information in the Hostname mismatch error, where the explanation part says that the certificates are issued to subjects specified in the subject field. However, there is missing information

Code	Code description	Total (37;33)	Expired certificate (14;13)	Hostname mismatch (15;14)	Unhandled crit. extension (8;6)	Representative quote
TooLong	It is too long, it contains too much information.	16	5	7	4	"Too much information. No minimalism concept is applied" (Error 1)
ExtraExplanation	Explanation part is too long or not needed at all.	5	0	4	1	"Maybe a little shorter explanation could be better" (Error 2)
Repeating	The information is repeated.	3	0	2	1	"It repeats itself in places" (Error 2)
ExtraWhatToDo	What to do part is not needed.	3	0	3	0	"I don't think the 'what to do' section is needed [...]" (Error 2)

Table 5.6: Reasons for the bloat in the second documentation. The first number in the heading expresses how many respondents considered the second documentation bloated or rather bloated. The second number shows how many of them expressed their opinions on the bloat.

that the recommended way is to specify the subjects in the subject alternative name extension (incorrectness case).

A noteworthy observation is that people did not know where to write a comment for a flaw, so they sometimes wrote the same or very similar comment for more flaws. Most often, they wrote the same comments for incompleteness & ambiguity and bloated & tangled documentation. It implicates that these flaws were hard to distinguish for them and somehow similar in a heart.

5.7 Additional comments

Other remarkable comments included recommendations such as keeping the documentation short and simple (13 respondents) and adding some examples (4 respondents). Some useful suggestions are adding

Code	Code description	Total (33;29)	Expired certificate (15;14)	Hostname mismatch (12;11)	Unhandled crit. extension (6;4)	Representative quote
ExtraWhatToDo	What to do part is not needed (either whole part or just part for users/developers).	7	3	4	0	"The part for certificate maintainer should not be there in my opinion, he should already know what to do [...]" (Error 1)
MuchInfo	It contains too much information.	7	4	1	2	"Too much of a story for a simple thing" (Error 1)
ExtraSecPerspective	Security perspective part should be general for all errors or removed.	4	0	2	2	"The security perspective as a whole section is maybe too much. I would expect it for the extensions documentation in general, not for evry possible error." (Error 3)
ExtraConsequences	Consequences part is too long/useless.	3	2	1	0	"I find "Consequences" entirely redundant and useless." (Error 1)
ExtraInfo	Information about CRL, CA or public key is not needed.	3	2	1	0	"It explained what a certificate holder is with mentioning the public key but this is an detail that is not needed." (Error 2)

Table 5.7: Reasons for the tangled information in the second documentation. The first number in the heading expresses how many respondents considered the second documentation tangled or rather tangled. The second number shows how many of them expressed their opinions on the tangled.

a link for lengthy documentation or other resources, adding a link to a protocol or RFC, including debugging information, such as shell commands or some steps for debugging purposes. Also, what to do part could contain exact steps on how to fix the problem. Since the documentation looks long, the text could be hidden and shown after clicking on the particular part. Another advice is to keep general information in a general section and does not include it for every error.

6 Useful tips for writing the documentation

This chapter presents recommendations for writing the documentation for the errors for IT professionals, based on the survey results and Section 3.3.

1. **Short description.** It is essential to provide a short description of the problem. Ideally, one sentence should be enough. It is aimed at experienced users who need to receive the principal information, without forcing them to read all the text for less experienced users to find the heart of the problem.

2. **What to do.** The users need to know what to do when an error occurs. It includes not only a list of all available possibilities and suggestions but also exact steps on how to perform them. If possible, debugging information, such as command-line instructions on how to find more details needed to resolve the problem, should be involved.

3. **Explanation.** It is convenient to explain the reason and the root cause of the error, together with the background. It should not be very detailed, but it should give context to a user so (s)he is more capable of resolving the problem in the right way. In addition, it is useful to include field names from the certificate, which are affected and provide an explanation of those fields, as well as an explanation of the terms used through the documentation.

4. **Brevity.** Provide all needed information, but be as brief as possible. People do not have time (and will) to read long texts. Moreover, it is more probable that people will read a short text than a long text.

5. **Hide longer texts.** As mentioned, people tend to skip reading long texts. Show only primary information, such as short description and all possible sections. Show the information contained in a particular section on demand, e.g., after clicking on a button for expanding of that part.

6. **Structure.** Use an organized structure, which simplifies orientation in the documentation. Suitable can be outlined, bulleted or numerical format.

7. **Linguistic properties.** It is better to use short sentences. Avoid complicated wording. Do not use sophisticated grammatical constructs, for example, conjunctions, which prolong the sentences or grammatical tenses, which complicate the understanding.

7 Conclusion

The thesis aimed to propose and evaluate a new variant of documentation for certificate validation errors and compare it with the current documentation. I created documentation for three different errors. The errors were chosen to represent various levels of understanding and occurrence in reality. For evaluation of the design of the proposed documentation and comparing it to the current documentation, I prepared a questionnaire with both types of documentation and delivered it during an international open-source conference, where I got 190 valid answers.

The results showed that the majority of respondents (88.7%) prefer the new documentation for all three types of errors. On average, they prefer 22 lines of documentation, which approximately corresponds to the number of lines of proposed documentation, which had 23 to 27 lines. It indicates that the length of the new documentation was more or less fine for them. However, the first look at the documentation could discourage them from reading. Thus, the text should be wrapped in the sections and showed on-demand. At the same time, error code and short description, as they are in the current documentation, are also essential in the longer documentation. These parts are the most appreciated by experienced users, who need to know what is going on without the necessity to read the long text to find the required information.

Importantly, self-evaluation of the respondents showed that the new documentation helped them to understand the error better, which will, hopefully, have a positive impact on them when resolving the problem.

The participants perceived the current documentation mainly incomplete (61.6%) and ambiguous (36.9%). However, incompleteness was much less reported for Expired certificate error than for the other two errors. The reason is that the Expired certificate error is quite common and easy to understand.

The newly proposed documentation was considered mainly bloated (20.3%) and tangled (18.1%). Remarkable is the difference in the percentage of people for perceiving the most numerous flaw in both documentations – only one-fifth for bloat in the new documentation

compared to the three-fifths for incompleteness in the current documentation.

To sum up, the results show that people appreciate the new documentation, and the effort in creating better documentation makes a sense. Future work includes writing the documentation for all certificate validation errors based on the results of this thesis.

Bibliography

1. OPPLIGER, Rolf. *Contemporary Cryptography*. Artech House, Inc., 2005. ISBN 9781580536424.
2. MARTIN, K.M. *Everyday Cryptography: Fundamental Principles and Applications*. OUP Oxford, 2012. ISBN 9780199695591.
3. DAVIES, Joshua. *Implementing SSL/TLS using cryptography and PKI*. John Wiley and Sons, 2011. ISBN 9780470920411.
4. COOPER, David; SANTESSON, Stefan; FARRELL, Stephen; BOEYEN, Sharon; HOUSLEY, Russell; POLK, W Timothy. *Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* [Internet Requests for Comments]. 2008. Available from DOI: 10.17487/RFC5280. RFC. RFC Editor.
5. VACCA, John R. *Computer and information security handbook*. Newnes, 2012. ISBN 9780123943972. Available from DOI: 10.1016/B978-0-12-394397-2.00106-9.
6. DENT, Alex W; MITCHELL, Chris J. *User's Guide To Cryptography And Standards*. Artech House, Inc., 2004. ISBN 9781580535304.
7. LIPPERT, Marcus; KARATSIOLIS, Vangelis; WIESMAIER, Alexander; BUCHMANN, J. Life-cycle management of X. 509 certificates based on LDAP directories. *Journal of Computer Security*. 2006, vol. 14, no. 5, pp. 419–439. Available from DOI: 10.3233/JCS-2006-14503.
8. *X.509 Certificates and Certificate Revocation Lists (CRLs)*. 2020 [cit. 2020-04-26]. Available from: https://docs.oracle.com/javase/8/docs/technotes/guides/security/cert3.html.
9. PARASHAR, Ajay Raj; MITTAL, Deepti. *Cryptography and Network Security*. Laxmi Publications Pvt Ltd., 2015. ISBN 9789351382669.
10. VACCA, John R. *Cyber Security and IT Infrastructure Protection*. Syngress, 2014. ISBN 9780124166813.
11. CROSS, Michael. *Security+ Study Guide*. Syngress, 2007. ISBN 9781597491532.

12. NEMEC, Matus; KLINEC, Dusan; SVENDA, Petr; SEKAN, Peter; MATYAS, Vashek. Measuring Popularity of Cryptographic Libraries in Internet-Wide Scans. In: *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, 2017, pp. 162–175. Available from DOI: 10.1145/3134600.3134612.

13. *2.1 Downloading and installing* [cit. 2020-04-02]. Available from: https://gnutls.org/manual/html_node/Downloading-and-installing.html.

14. *Making X.509 errors usable.* 2020 [cit. 2020-04-02]. Available from: https://x509errors.org/.

15. UKROP, Martin; KRAUS, Lydia; MATYAS, Vashek; WAHSHEH, Heider Ahmad Mutleq. Will you trust this TLS certificate?: perceptions of people working in IT. In: *Proceedings of the 35th Annual Computer Security Applications Conference*. 2019, pp. 718–731. Available from DOI: 10.1145/3359789.3359800.

16. UDDIN, Gias; ROBILLARD, Martin P. How API documentation fails. *IEEE Software*. 2015, vol. 32, no. 4, pp. 68–75. Available from DOI: 10.1109/MS.2014.80.

17. BIDDLE, Robert; VAN OORSCHOT, Paul C; PATRICK, Andrew S; SOBEY, Jennifer; WHALEN, Tara. Browser interfaces and extended validation SSL certificates: An empirical study. In: *Proceedings of the 2009 ACM workshop on Cloud computing security*. 2009, pp. 19–30. Available from DOI: 10.1145/1655008.1655012.

18. FELT, Adrienne Porter; AINSLIE, Alex; REEDER, Robert W; CONSOLVO, Sunny; THYAGARAJA, Somas; BETTES, Alan; HARRIS, Helen; GRIMES, Jeff. Improving SSL warnings: Comprehension and adherence. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2015, pp. 2893–2902. Available from DOI: 10.1145/2702123.2702442.

19. SUNSHINE, Joshua; EGELMAN, Serge; ALMUHIMEDI, Hazim; ATRI, Neha; CRANOR, Lorrie Faith. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In: *USENIX security symposium*. 2009, pp. 399–416.

20. BAUER, Lujo; BRAVO-LILLO, Cristian; CRANOR, Lorrie Faith; FRAGKAKI, Elli. *Warning Design Guidelines*. 2013. Available also from: `https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab13002.pdf`. Technical report. Carnegie Mellon University.

21. BRAVO-LILLO, Cristian; CRANOR, Lorrie Faith; DOWNS, Julie; KOMANDURI, Saranga; SLEEPER, Manya. Improving computer security dialogs. In: *IFIP Conference on Human-Computer Interaction*. 2011, pp. 18–35. Available from DOI: `10.1007/978-3-642-23768-3_2`.

22. WOGALTER, Michael S; CONZOLA, Vincent C; SMITH-JACKSON, Tonya L. Research-based guidelines for warning design and evaluation. *Applied ergonomics*. 2002, vol. 33, no. 3, pp. 219–230. Available from DOI: `10.1016/S0003-6870(02)00009-1`.

23. REEDER, Rob; KOWALCZYK, E Cram; SHOSTACK, Adam. Helping engineers design NEAT security warnings. In: *Proceedings of the Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA*. 2011.

24. LAUGHERY, Kenneth R; WOGALTER, Michael S. A three-stage model summarizes product warning and environmental sign research. *Safety science*. 2014, vol. 61, pp. 3–10. Available from DOI: `10.1016/j.ssci.2011.02.012`.

25. HARBACH, Marian; FAHL, Sascha; YAKOVLEVA, Polina; SMITH, Matthew. Sorry, I don't get it: An analysis of warning message texts. In: *International Conference on Financial Cryptography and Data Security*. 2013, pp. 94–111. Available from DOI: `10.1007/978-3-642-41320-9_7`.

26. *Coding Qualitative Data: How to Code Qualitative Research*. 2020 [cit. 2020-05-10]. Available from: `https://getthematic.com/insights/coding-qualitative-data/`.

A Documentation

Documentation variant number 1

X509_V_ERR_CERT_HAS_EXPIRED
The certificate has expired: that is the notAfter date is before the current time.

X509_V_ERR_HOSTNAME_MISMATCH
Hostname mismatch.

X509_V_ERR_UNHANDLED_CRITICAL_EXTENSION
Unhandled critical extension.

Documentation variant number 2

X509_ERR_CERT_HAS_EXPIRED
Validity of the certificate has expired.

Explanation
Every certificate is delivered for a certain time period (determined by notBefore and notAfter fields in certificate). The time period determines the validity of certificate. When time period elapses, the certificate becomes expired.

Security perspective
The certificate is not valid anymore which means that issuing Certification Authority (CA) does not maintain information about the certificate and does not guarantee the correctness of information provided in the certificate. Moreover, expired certificates are removed from Certificate Revocation Lists (CRLs) which means that a certificate might be revoked in the past (e.g. because of revealed private key), but we do not get this information about expired certificate.

What to do
Ensure that date, time and time zone are set correctly on your device. If the time settings are correct and you are responsible for the certificate, you should get new valid certificate from the CA. In this case, contact either the CA which issued the previous certificate or another CA. If the time settings are correct and you are not responsible for the certificate, contact responsible person. If it is a web page with expired certificate, do not provide any personal or secret information to this site.

Consequences
If you are responsible for the certificate and you decide not to renew it, the expired certificate is untrustworthy and your clients do not have to trust you or your business. If you are not responsible for the certificate and you decide to trust to it, you may communicate with another person/entity than you think which may lead to theft of personal information.

X509_ERR_HOSTNAME_MISMATCH
The requested hostname does not match the subject name in the certificate.

Explanation
The subject field in the certificate carries information about the certificate's holder (an entity that is associated with the certificate's public key). Certificates are issued to subjects specified in the subject field. It is also this case – the certificate was issued to the subject specified in the certificate. However, the problem is that the subject name is different than the server hostname – the server has a certificate which is not associated with the server, the certificate was issued for another server.

Security perspective
The server pretends to be another server. It can be caused by an attacker who may want to steal your information shared with the server (e.g., username and password). Another reason can be a misconfiguration of the server or incomplete information in the certificate.

What to do
If you are responsible for the certificate, check whether all possible hostnames are listed in the certificate, either in the subject name or in the subject alternative name (e.g., 'example.com' and also 'www.example.com'). Another possibility is to redirect all associated traffic to the hostname indicated in the subject name (e.g., redirect 'example.com' to 'www.example.com'). If you are not responsible for the certificate, contact the responsible person. Try to type full site name, including www. If the problem persists, do not provide any personal or secret information to this site.

Consequences
If you access another server than you think, you may receive wrong or malicious content. Moreover, all information provided to this server can be misused.

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.

B Questionnaire

Documentation variant number 1

Instructions
Imagine that you are a developer, and you are working with a protocol that makes use of X.509 certificates. While trying to use the protocol, an X.509 error is displayed, so you open documentation for the error…

Now you will be gradually shown two variants of documentation for an X.509 error. Please, answer the questions concerning each documentation variant.

[Documentation variant number 1 (see appendix A) was displayed here]

1. Have you seen this error before?
   {Yes; No; I do not remember}
2. Do you understand the error?
   {Yes; Rather yes; Rather no; No}
3. How much are you satisfied with the documentation for the error?
   {Extremely satisfied; Very satisfied; Moderately satisfied; Slightly satisfied; Not at all satisfied}
4. How much was the documentation helpful?
   {Extremely helpful; Very helpful; Moderately helpful; Slightly helpful; Not at all helpful}
5. For each of the following possible documentation flaws, decide whether you agree or not.

   (a) Do you consider the documentation for the error **incomplete**?
   (*Incompleteness = Some information is missing in the documentation.*)

(b) Do you consider the documentation for the error **ambiguous**?
(*Ambiguity = The description was mostly complete but unclear.*)

(c) Do you consider the documentation for the error **inconsistent**?
(*Inconsistency = The documentation of elements meant to be combined didn't agree.*)

(d) Do you consider the documentation for the error **incorrect**?
(*Incorrectness = Some information was incorrect.*)

(e) Do you consider the documentation for the error **bloated**?
(*Bloated = The description was verbose or excessively extensive.*)

(f) Do you consider the documentation for the error **tangled**?
(*Tangled = The description was tangled with information the respondent didn't need.*)

{Yes; Rather yes; Rather no; No}

6. Why do you consider the documentation for the error **incomplete**?
(*Incompleteness = Some information is missing in the documentation.*)
[Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 5a]

7. Why do you consider the documentation for the error **ambiguous**?
(*Ambiguity = The description was mostly complete but unclear.*)
[Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 5b]

8. Why do you consider the documentation for the error **inconsistent**?
(*Inconsistency = The documentation of elements meant to be combined didn't agree.*)

[Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 5c]

9. Why do you consider the documentation for the error **incorrect**?
(*Incorrectness = Some information was incorrect.*)
[Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 5d]

10. Why do you consider the documentation for the error **bloated**?
(*Bloated = The description was verbose or excessively extensive.*)
[Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 5e]

11. Why do you consider the documentation for the error **tangled**?
(*Tangled = The description was tangled with information the respondent didn't need.*)
[Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 5f]

Documentation variant number 2

Instructions
Now imagine the same situation: you are a developer, and you are working with a protocol that makes use of X.509 certificates. While trying to use the protocol, an X.509 error is displayed, but now you get the documentation variant shown below.

[Documentation variant number 2 (see appendix A) was displayed here]

1. Do you understand the error after reading the documentation for the error?
{Yes; Rather yes; Rather no; No}

2. How much are you satisfied with the documentation for the error?
{Extremely satisfied; Very satisfied; Moderately satisfied; Slightly satisfied; Not at all satisfied}

3. How much was the documentation helpful?
   {Extremely helpful; Very helpful; Moderately helpful; Slightly helpful; Not at all helpful}

4. For each of the following possible documentation flaws, decide whether you agree or not.

   (a) Do you consider the documentation for the error **incomplete**?
   (*Incompleteness = Some information is missing in the documentation.*)

   (b) Do you consider the documentation for the error **ambiguous**?
   (*Ambiguity = The description was mostly complete but unclear.*)

   (c) Do you consider the documentation for the error **inconsistent**?
   (*Inconsistency = The documentation of elements meant to be combined didn't agree.*)

   (d) Do you consider the documentation for the error **incorrect**?
   (*Incorrectness = Some information was incorrect.*)

   (e) Do you consider the documentation for the error **bloated**?
   (*Bloated = The description was verbose or excessively extensive.*)

   (f) Do you consider the documentation for the error **tangled**?
   (*Tangled = The description was tangled with information the respondent didn't need.*)

   {Yes; Rather yes; Rather no; No}

5. Why do you consider the documentation for the error **incomplete**?
   (*Incompleteness = Some information is missing in the documentation.*)
   [Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 4a]

6. Why do you consider the documentation for the error **ambiguous**?
   (*Ambiguity = The description was mostly complete but unclear.*)
   [Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 4b]

7. Why do you consider the documentation for the error **inconsistent**?
   (*Inconsistency = The documentation of elements meant to be combined didn't agree.*)
   [Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 4c]

8. Why do you consider the documentation for the error **incorrect**?
   (*Incorrectness = Some information was incorrect.*)
   [Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 4d]

9. Why do you consider the documentation for the error **bloated**?
   (*Bloated = The description was verbose or excessively extensive.*)
   [Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 4e]

10. Why do you consider the documentation for the error **tangled**?
    (*Tangled = The description was tangled with information the respondent didn't need.*)
    [Free text; the question was displayed only if answer was 'Yes' or 'Rather yes' at question 4f]

11. How important do you consider these parts of the documentation for this error?

    (a) Error code name (written in capitals)

    (b) Short description (follows error code name)

    (c) Explanation

    (d) Security perspective

(e) What to do

(f) Consequences

{Extremely important; Very important; Moderately important; Slightly important; Not at all important}

12. Would you shorten the last documentation for the error by removing a part/some parts of it? Please, choose all the appropriate options.
{Yes, by removing error code name (written in capitals); Yes, by removing short description (follows error code name); Yes, by removing Explanation part; Yes, by removing Security perspective part; Yes, by removing What to do part; Yes, by removing Consequences part; No}

13. Which documentation of the error do you prefer?
{The first one (the short one); The second one (the long one)}

14. Why do you prefer the first documentation for the error?
[Free text; the question was displayed only if answer was 'The first one (the short one)' at question 13]

15. Why do you prefer the second documentation for the error?
[Free text; the question was displayed only if answer was 'The second one (the long one)' at question 13]

16. How many lines of documentation would you prefer for the error? (The documentation above has X[1] lines.)
[Number answer]

17. Any comment regarding understanding or improving documentation for the errors?
[Free text]

General part

Please, answer the last few general questions.

1. X was replaced with the number of lines for the displayed documentation – 27 lines for Expired certificate error, and 23 lines for Hostname mismatch error and Unhandled critical extension error

1. Gender
   {Man; Woman; Other}

2. Are you currently a student of IT-related discipline?
   {Yes; No}

3. What is your highest reached degree in IT related discipline?
   {None; Bachelor degree (e.g. Bc.); Master degree (e.g. Mgr., Ing.); Postgraduate degree (e.g. RNDr., PhD.)}

4. How many years have you been employed in the IT field (including part-time jobs and internships)?
   [Number answer]

5. What is your current IT position? (If you are a student and employed at the same time, refer to your job position.)
   {Developer, Software Engineer; Software Architect; Tester, Quality Assurance Engineer; Security Specialist; Network Specialist; Database Specialist; UX Designer; Technical Writer; IT Support, Help Desk Specialist; Product Manager; Manager; Academic Researcher; Student; Other}

6. In which country did you spend most of your working life (consider only IT-related work)? (If you are a student, refer to your student life related to IT.)
   [Drop-down list with all the countries]

7. How do you consider your knowledge of computer security in general?
   {Excellent; Very good; Good; Fair; Poor}

8. How do you consider your knowledge of X.509 certificates?
   {Excellent; Very good; Good; Fair; Poor}

9. How many times have you used the OpenSSL library? Consider both CLI (Command-Line Interface) and usage in the source code.
   {More than 5 times; 2 - 5 times; Once; Never}