

MASARYK UNIVERSITY
FACULTY OF INFORMATICS



Security and cryptography in GO

BACHELOR'S THESIS

Lenka Svetlovská

Brno, Spring 2017

Replace this page with a copy of the official signed thesis assignment and a copy of the Statement of an Author.

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.

Lenka Svetlovská

Advisor: RNDr. Andriy Stetsko, Ph.D.

Acknowledgement

I would like to thank RNDr. Andriy Stetsko, Ph.D. for the management of the Bachelor thesis, valuable advice, and comments. I would also like to thank the consultant from Y Soft Corporation a.s., Mgr. Lenka Bačinská, for useful advice, dedicated time and patience in consultations and application development.

Likewise, I thank my family and friends for their support throughout my studies and writing this thesis.

Abstract

The aims of the thesis are twofold.

First, the thesis overviews and compares cryptographic libraries available for Go programming language.

Second, the thesis contains the implementation, tests and evaluation of a prototype of a client application able to generate asymmetric keys and certificate signing requests, connect to a server application using TLS_PSK (pre-shared key) cipher suite.

Keywords

Security, Certificate, TLS, TLS_PSK, Pre-shared key, Language Go,
Language C, Cgo, OpenSSL

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 1 |
| 2 | Basic Terms | 3 |
| 2.1 | <i>Certificate</i> | 3 |
| 2.1.1 | Standard X.509 | 3 |
| 2.1.2 | Certificate Authority | 3 |
| 2.1.3 | Self-signed Certificate | 4 |
| 2.1.4 | Certificate Signing Request | 5 |
| 2.1.5 | Formats PEM and DER | 5 |
| 2.2 | <i>Protocol SSL/TLS</i> | 6 |
| 2.2.1 | PSK Key Exchange Algorithm | 8 |
| 3 | Language Go | 11 |
| 3.1 | <i>Introduction</i> | 11 |
| 3.2 | <i>How to Start</i> | 11 |
| 3.2.1 | Installation | 11 |
| 3.2.2 | Environment | 12 |
| 3.2.3 | Compilation and Arguments | 12 |
| 3.3 | <i>Packages</i> | 13 |
| 3.4 | <i>C? Go? Cgo!</i> | 14 |
| 4 | Go Packages Analysis | 17 |
| 4.1 | <i>Cryptographic functions</i> | 17 |
| 4.2 | <i>Expansion measures</i> | 20 |
| 5 | Implementation | 23 |
| 5.1 | <i>Assignment</i> | 23 |
| 5.2 | <i>TLS_PSK</i> | 23 |
| 5.2.1 | Raff | 23 |
| 5.3 | <i>Language C in Go</i> | 24 |
| 5.3.1 | Initialization | 24 |
| 5.3.2 | Connection | 24 |
| 5.3.3 | Reading from and writing to server | 25 |
| 5.4 | <i>Using C-methods in Go</i> | 25 |
| 5.5 | <i>Communication protocol</i> | 25 |
| 5.5.1 | Connection using TLS_PSK | 26 |

| | | |
|----------|---|-----------|
| 5.5.2 | Protocol version exchange | 26 |
| 5.5.3 | Key length | 26 |
| 5.5.4 | Certificate signing | 27 |
| 5.5.5 | Achieving trust | 28 |
| 5.6 | <i>Compilation and run</i> | 28 |
| 6 | Evaluation | 29 |
| 6.1 | <i>Select Libraries</i> | 29 |
| 6.2 | <i>OpenSSL and Language C</i> | 29 |
| 6.3 | <i>Testing</i> | 30 |
| 6.3.1 | Connectivity test | 30 |
| 6.3.2 | Step by step testing of communication | 30 |
| 6.3.3 | File test | 31 |
| 7 | Conclusion | 33 |

List of Tables

- 4.1 Table of cryptographic libraries in Go 18
- 4.2 Filtered table of packages with expansion measures 21

List of Figures

- 2.1 Structure X.509 Certificate 4
- 2.2 A sample example of certificate view 6
- 2.3 TLS_PSK Key Exchange, edited from [11] 9

1 Introduction

One of the oldest systems of symmetric cryptography is probably “*Skytale*” used in 5th century BC. The secret was made by the stick with some diameter which was reeled leather stripe on so that covered surface of the stick. The message was written there, and after the untangled, the text was unreadable. Cryptography informs as we know nowadays, it began to develop at the beginning of 20th century especially with development telegraphs. Using cryptography happened necessary part of ordinary life. All connections through we communicate are secured by some case through cryptographic functions. An only little mistake in those functions can cause to misuse private data.

Programming language Go belongs to languages which the main idea is provided the best tools for programmers work even though it is not always the easiest or the most effective way. Language Go was made by Google Inc. company in 2007, and it has syntax derived from language C. Safety, speed and concurrency are his main characters. Go provides extensive options for cryptography such as ciphering, hashing and work with certificates.

The aims of the thesis are twofold. First, it is necessary to examine features of language Go related safety and cryptography, analyze libraries which Go contains and also search for available third-party libraries. The thesis contains the overview, evaluate and compare existing cryptographic liberates based on their license, usability, supported cryptographic functions, such as symmetric and asymmetric encryption and hash functions. Next based on possibilities for the generation of cryptographic keys, work with X.509, such as generation of self-signed certificates, support for certificate signing requests and support for different formats and extensions. It also compares support of higher level protocols such as SSL/TLS.

Second, the thesis contains the implementation in language Go, tests and evaluation of a prototype of a client application able to generate asymmetric keys and certificate signing requests and connect to a server application using TLS_PSK.

The Bachelor thesis is consulted and realized in collaboration with Y Soft Corporation, a.s.

2 Basic Terms

In this chapter, I will define the basic terms which are necessary to the understanding of the text presented in the following sections. First I will describe the structure of certificates, standard X.509, certificate authority and signing process. I will explain self-signed certificate and formats. Finally, I will describe protocols SSL/TLS and TLS pre-shared key (TLS_PSK) algorithm used in the application.

2.1 Certificate

The certificate is digitally signed data structure whose basis includes a public key of certificate owner. There are some standards of the certificate structure (X.509, EDI, WAP, etc.). The Internet is based on standard X.509 version 3, which was issued by the ITU [1].

2.1.1 Standard X.509

Standard X.509 was originally designed as an authentication framework for X.500 directories. They have a hierarchical structure, and the individual attributes can be assigned to individual computers of companies or individual printers [2]. Certificate X.509, see Figure 2.1.

2.1.2 Certificate Authority

The Certificate Authority (CA) is an independent third party which issues certificates.

In other words, the CA is an institution that inspects the certificate request and issues whose validity is verifiable using the responsive public key. The CA was created to ensure secure encryption through a certified public key and guarantee the validity of the digital signature. The CA also provides their validity revocation. The CA is truly credible, must be impartial and, if it is possible, should be subordinate to any higher CA. Subordination means that it identifies the usage of certificates signed by the higher certificate authority [1].

Root CAs, certificate authorities at the highest level, use the certificate signed by themselves (self-signed certificate).

2. BASIC TERMS

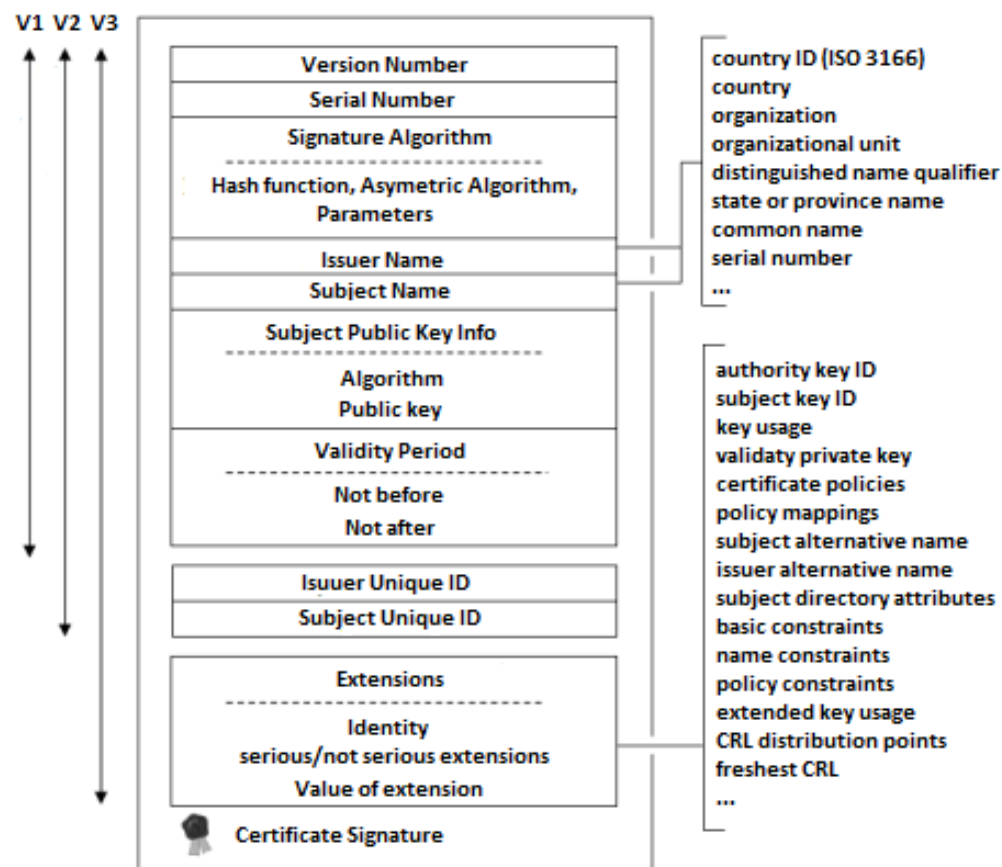


Figure 2.1: Structure X.509 Certificate

2.1.3 Self-signed Certificate

The self-signed certificate is a certificate which the applicant issues by himself. The self-signed certificate has the same data structure as a certificate issued by CA. This certificate is recognized according to same item Subject and item Issuer.

As proof of the private key possession by the user, the self-signed certificate uses a digital signature which was made by the private key belonging to the public key in the certificate. Verification of the signature is carried out through a public key in the actual certificate [1].

2.1.4 Certificate Signing Request

The certificate applicant can apply CA to sign certificate by submitting a data structure called a certificate request (CSR) [1]. The most common format is PKCS#10. The CSR should include:

- Applicant ID
- The public key
- Evidence of the possession of the private key
- Other information that the user wishes to insert certificate
- May contain evidence of the generation of paired data
- Data necessary for billing (in case issuance of certificates is paid)
- Passwords for communication with CA:
 - One-time password for issuing the certificate
 - One-time password for certificate revocation
 - Permanent password for personal (non-electronic) communication between user and CA
 - Phrase (in case losing all passwords)

The certificate authority must fill individual fields of the certificate before it signs the result digitally. The CA takes CSR, checks completed fields, and fills two important fields called validity period - the time while the certificate is valid - which are shown as: not before, not after. The CA can also add extensions, such as Subject Alternative Name, information about CA, etc. (see figure 2.1).

2.1.5 Formats PEM and DER

The PEM (Privacy Enhanced Mail) is a Base64 encoded DER certificate. It is designed to be safe for inclusion in ASCII or even rich-text documents. This means that we can just copy and paste the content of a pem file to another document and back. The following figure is a sample PEM file containing a private key and a certificate 2.2.

A certificate or key must start with the header where the number of dashes is meaningful and must be correct. A single PEM file can contain a number of certificates and a key, for example, a single file with a public certificate, intermediate certificate, root certificate or private key [4].

2. BASIC TERMS

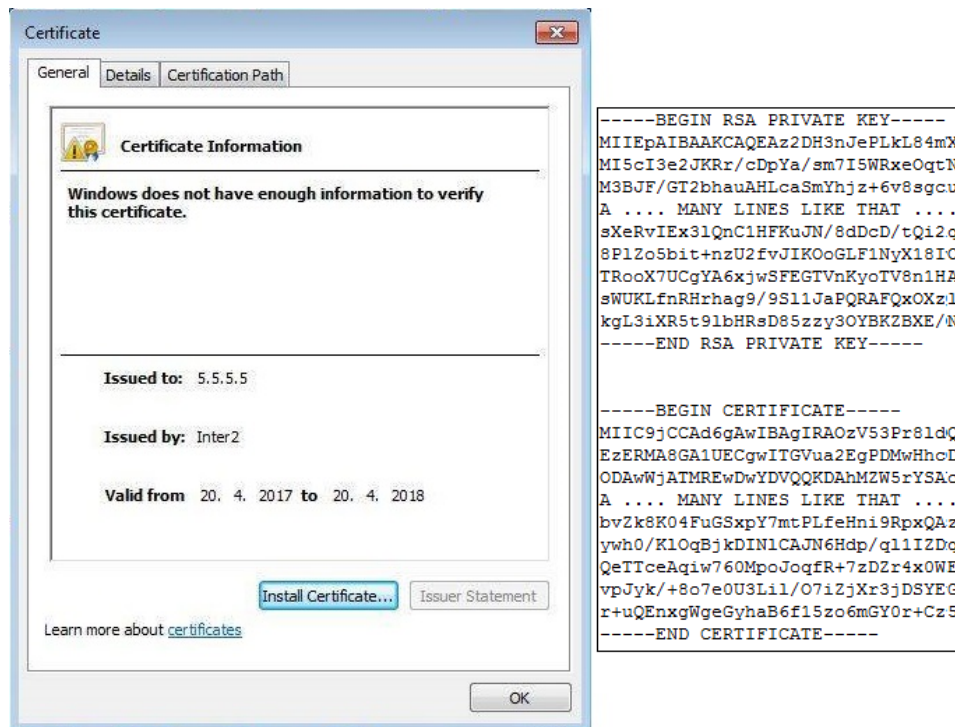


Figure 2.2: A sample example of certificate view

The DER (Distinguished Encoding Rules) is a binary form of ASCII PEM format certificate. All types of certificates and private keys can be encoded in DER format; its information is stored in the binary DER for ASN.1 and applications providing RSA, SSL and TLS should handle DER encoding to read the information. DER can not contain more than one certificate [5].

2.2 Protocol SSL/TLS

Protocol SSL/TLS is used for communication security between the client and the server. It creates a framework for the use of encryption and hash functions.

Protocol SSL was developed by Netscape Communications which published three versions. The first version was only a test; the second has been used in practice. However, it still contained security

vulnerabilities; the most important was susceptibility to attack *man in the middle* [6]. The third version was introduced in 1996, and its specification could be found in the document *The SSL Protocol Version 3.0* [7]. From this release was created TLS protocol which is currently the most widespread and supported [6]. There are currently three versions which have only minimal differences. TLS version 1.3 is a draft already used in multiple locations [8]. For example, the forthcoming *OpenSSL 1.1.1* release will include support for *TLSv1.3* [9].

Protocol SSL/TLS provides authentication of the two communicating parties by using asymmetric encryption, message integrity by using MAC and confidentiality by encrypting all communications by selected symmetric cipher.

Protocol SSL/TLS is located between the application and the transport layer reference ISO/OSI model and consists of two main parts. They are *The Record Layer Protocol* and *Handshake Protocol* [6].

Record Layer Protocol (RLP)

RLP processes application data, performs fragmentation, compression and data encryption. On the other hand, it decrypts the data again and verifies the checksums. RLP does not care about the type of encryption algorithm or encryption key setting. This information is from HP.

Handshake Protocol (HP)

HP is activated immediately after establishment the connection and provides identification of communicating parties, negotiation of cryptographic algorithms, compression algorithms and other attributes. Then it creates a *master secret* from which are derived encryption keys, initiation vectors, and the MAC. The process of the protocol is:

1. The client sends a *ClientHello* message to the server, along with the client's random value and supported cipher suites.
2. The server responds by sending a *ServerHello* message to the client, along with the server's random value.
3. The server sends its certificate to the client for authentication and may request a certificate from the client. The server sends the *ServerHelloDone* message.

2. BASIC TERMS

4. If the server has requested a certificate from the client, the client sends it.
5. The client creates a random *Pre-Master Secret* and encrypts it with the public key from the server's certificate, sending the encrypted *Pre-Master Secret* to the server.
6. The server receives the *Pre-Master Secret*. The server and client each generate the *Master Secret* and session keys based on the *Pre-Master Secret*.
7. The client and the server exchange the *Finished* messages.

Client and server can now exchange application data over the secured channel they have established. All messages sent from client to server and from server to client are encrypted using session key [10].

2.2.1 PSK Key Exchange Algorithm

The cipher suites with the PSK key exchange algorithm use only symmetric key algorithms and are particularly suitable for performance-constrained environments where both ends of the connection can be controlled. The cipher suites are intended for a rather limited set of applications, usually involving only a very small number of clients and servers.

1. The client indicates to use pre-shared key authentication by including one or more PSK cipher suites in the *ClientHello* message.
2. If the TLS server also wants to use pre-shared keys, it selects one of the PSK cipher suites and places it in the *ServerHello* message. The server can provide a "PSK identity hint" in the *ServerKeyExchange* message. If no hint is provided, the *ServerKeyExchange* message is omitted.
3. The client indicates which key to use by including a "PSK identity" in the *ClientKeyExchange* message.
4. The *Certificate* and *CertificateRequest* payloads are omitted from the response.

5. The TLS handshake is authenticated using the *Finished* messages.

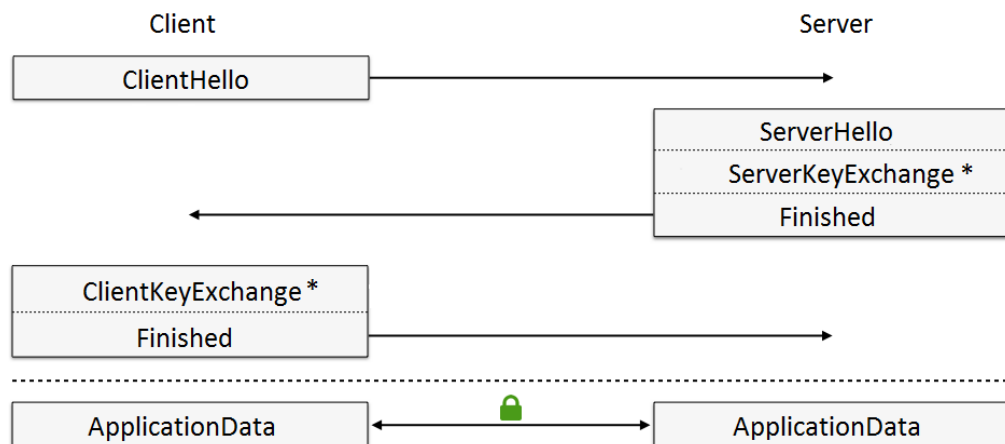


Figure 2.3: TLS_PSK Key Exchange, edited from [11]

If the server does not recognize the PSK identity, it may respond with an *unknown_psk_identity* alert message. Alternatively, if the server wishes to hide the fact that the PSK identity was not known, it may continue the protocol as if the PSK identity existed, but the key was incorrect: that is, respond to an *decrypt_error alert* [12].

3 Language Go

In this chapter, I will explain the main characters of language Go and show how to write the code. Next, I will describe Go libraries called packages and the tool Cgo.

3.1 Introduction

Go is a programming language developed at *Google* in the year 2007 and announced in November 2009. Many companies have started using Go because of its performance, simplicity, ease of use and powerful tooling. Go programming language is a statically-typed language with advanced features and a clean syntax [13]. It combines the performance and security benefits associated with using a compiled language like C++ with the speed of a dynamic language like *Python*. It provides:

- garbage collector - memory is cleaned up automatically when nothing refers to it anymore,
- fast compilation time - through effective work with additions individual parts of the program and simple grammar,
- light-weight processes (via go-routines), channels,
- a rich standard library,
- easy testing - incorporated directly into the core language,
- one of the best documentation - a clear and full of examples.

Go excluded some features intentionally to keep language simple and concise. There is no support for type inheritance, method or operator overloading, circular dependencies among packages, pointer arithmetic, assertions nor for generic programming.

3.2 How to Start

3.2.1 Installation

Golang, the go official website, provides the installer of Go to download free for Windows, Linux, Mac OS X and FreeBSD. To confirm everything is working, open a terminal and type the following:

```
1 go version
```

3. LANGUAGE GO

Upgrading from an older version of Go must be predeceased by removing the existing version.

3.2.2 Environment

After installation, it is necessary to set Go to the `$PATH` environment variable and set the `$GOROOT` environment variable to point to the directory in which it was installed. The Go toolset uses an environment variable called `$GOPATH` to find Go source code.

For example, if you installed Go to your home directory you should add commands like the following to `$HOME/.profile`:

```
1 export GOROOT=$HOME/go1.X
2 export PATH=$PATH:$GOROOT/bin
3 export GOPATH=$HOME/Projects/go
```

`$GOPATH` has to contain directories `src` and `pkg`.

3.2.3 Compilation and Arguments

Go is a compiled language, and like many languages, it makes heavy use of the command line. Open up a new terminal, set up directory where you saved your file and type in the following for run the file:

```
1 go run <file -name>.go
```

or type in the following to parameterize execution of programs. First must be used go build command to create a binary program.

```
1 go build <file -name>.go
2 ./<file -name> <arguments>
```

In code, `os.Args` provides access to raw command-line arguments. The first value is the path to the program, and `os.Args[1:]` holds the arguments to the program.

```
1 argsWithProg := os.Args
2 argsWithoutProg := os.Args[1:]
3 arg := os.Args[3]
```

Do not forget to import package `os`.

3.3 Packages

In Go, source files are organized into system directories called packages. To develop software applications, writing maintainable and reusable pieces of code is very important. Go provides the modularity and code reusability through its package system. Go encourages programmers to write small pieces of software components through packages, and compose their applications with these small packages.

The packages from the standard library are available at the *pkg* subdirectory of the `$GOROOT` directory. When we install Go, an environment variable `$GOROOT` will be automatically added to our system for specifying the Go installer directory. The Go developer community is very enthusiastic about developing third-party Go packages. When you develop Go applications, you can affect these third-party Go packages [15].

When programmers develop executable programs, they will use the package *main* for making the package as an executable program. The package *main* tells the Go compiler that the package should compile as an executable program instead of a shared library. When programmers build shared libraries, they will not have any main package and main function in the package.

To download third-party Go packages, the following command is used:

```
1 go get example/exampleLib
```

After installing the `exampleLib`, put the import statement in programs for reusing the code, as shown below:

```
1 package db
2 import (
3     "example/exampleLib"
4     "example/exampleLib/sub"
5 )
6 func init {
7     // initialization code here
8 }
```

Third-party Go packages are installed by using this command:

```
1 go install
```

The `go install` command will build the package “sub” which will be available at the *pkg* subdirectory of `$GOPATH`.

3. LANGUAGE GO

```
1 package main
2 import (
3     "fmt"
4     "example/exampleLib/sub"
5 )
6 func main() {
7     sub.Add("dr", "Dart")
8     fmt.Println(sub.Get("dr"))
9     // code here
10 }
```

3.4 C? Go? Cgo!

Cgo allows Go to interoperate with C code. Go source file imports "C", and it is immediately preceded by comment lines which may contain any C code, including function and variable declarations and definitions. It is necessary to say that there must be no blank lines in between the cgo comment and the import statement.

```
1 package main
2 /*
3 #include <stdio.h>
4
5 void hello() {
6     printf("Hello World!\n");
7 }
8 */
9 import "C"
10
11 func main() {
12     C.hello()
13 }
```

Cgo allows including own C libraries. The header file *foo.h*, the library implementation *foo.c* and go wrapper *foo.go* are located in the same package *\$GOPATH/src/foo*.

```
1 #cgo CFLAGS: -I/${$GOPATH}/src/foo
2 #cgo LDFLAGS: -L/${$GOPATH}/src/foo -lfoo
```

Go wrapper contains the explicit paths in the cgo flags because of an environment issue where *libfoo* wasn't found by the Go linker.

```
1 go install foo
```

By installing the package, everything is prepared for use in Go. Package is called in Go code through *import "foo"*.

In order to use Cgo on Windows, it is firstly needed to install a gcc compiler and have *gcc.exe* in *\$PATH* environment variable before compiling with Cgo will work.

4 Go Packages Analysis

This chapter contains the overview, evaluate and compare existing cryptographic libraries based on their measures and expansion measures important for implementation.

4.1 Cryptographic functions

It was necessary to examine features of language Go related to the security and cryptography, analyze libraries which Go contains and also search for available third-party libraries.

Table 4.1 shows analyzed Go package Crypto created by *Golang* and other Go packages created by third-parties. Individually items mean:

- Name - founder nickname (almost all packages are searched on <https://github.com/> where is not published real name of founder or contributors) and name of package.
- Cryptographic functions - support cryptographic functions, such as symmetric encryption, asymmetric encryption and hash functions (all/sym/asym/hash/unknown).
- Start of project - a year of creating project with package.
- Is still opened - the important measure is if contributors still work on the project (Yes/No).
- Issue tracker system - support of solving bugs, feature requests, tracking todos, and more (Yes/No).
- Documentation Accessibility - assessed on a scale of 0-5 points (5 is the highest) according to own experience to work with the package.
- Downloads - the number of downloads. In case the package is saved on <https://github.com/>, the information about downloads presents the value of Fork. Downloads of package Crypto created by Golang is unknown; this package is automatically installed with installing program Go.
- License - availability of licenses for free (Yes/Payment). The payment indicates the amount of payment per some period. This case did not occur.

4. GO PACKAGES ANALYSIS

Table 4.1: Table of cryptographic libraries in Go

| Name | Cryptc func- tions | Start of project | Is still openec | Issue tracker system | Doc. acces- sibility | Down- loads | License |
|---------------------------------|--------------------------|------------------------|-----------------------|----------------------------|----------------------------|----------------|---------|
| golang/ crypto | all | 2009 | Y | Y | 5 | - | Y |
| ory-am/ fosite | asym, hash | 2015 | Y | Y | 4 | 39 | Y |
| square/ go-jose | asym, sym | 2014 | Y | Y | 4 | 70 | Y |
| Shopify/ ejson | hash | 2014 | Y | Y | 3 | 22 | Y |
| mittchellh/ go- mruby | asym | 2014 | Y | Y | 4 | 19 | Y |
| Sermo Digital/ jose | all | 2015 | Y | Y | 4 | 28 | Y |
| mozilla/ tls- observatory | hash | 2014 | Y | Y | 4 | 31 | Y |
| square/ certigo | hash | 2016 | Y | Y | 3 | 12 | Y |
| docker/ libtrust | all | 2014 | N | Y | 4 | 26 | Y |
| dedis/ crypto | sym, hash | 2010 | Y | Y | 4 | 17 | Y |
| dchest/ blake2b | hash | 2012 | N | Y | 4 | 6 | Y |
| enceve/ crypto | hash | 2016 | N | Y | 4 | 1 | Y |
| Continued on next page | | | | | | | |

Table 4.1 – continued from previous page

| Name | Cryptc func- tions | Start of project | Is still openec | Issue tracker system | Doc. acces- sibility | Down- loads | License |
|---------------------------------|--------------------------|------------------------|-----------------------|----------------------------|----------------------------|----------------|---------|
| go-libp2p-crypto | all | 2015 | Y | Y | 4 | 5 | Y |
| dchest/blake2s | hash | 2012 | N | N | 3 | 3 | Y |
| benburkert/sym, openpgp hash | sym, hash | 2012 | N | N | 3 | 0 | Y |
| minio/sha256-simd | hash | 2016 | Y | Y | 3 | 14 | Y |
| avelino/awesome-go | un- known | 2014 | Y | Y | 2 | 2287 | Y |
| ethereum/go-ethereum | all | 2013 | Y | Y | 4 | 1028 | Y |
| chain/chain | hash | 2015 | Y | Y | 4 | 113 | Y |
| lightning-net-work/lnd | sym, hash | 2015 | Y | Y | 4 | 50 | Y |
| square/go-jose | asym, hash | 2014 | Y | Y | 4 | 70 | Y |
| dgrijalva/jwt-go | asym, hash | 2012 | Y | Y | 4 | 226 | Y |
| golang/oauth2 | asym, hash | 2014 | Y | Y | 4 | 279 | Y |

The table 4.1 was created based on information available on following websites [22] [23] [24] [25]. The table does not include packages which do not support any cryptographic functions. Also, the table does

not contain information from untrusted sources. During the analysis, I discovered sources which are not up to date or supported [26].

I searched immediately using keywords as names of functions or words in descriptions of functions. I found plenty of packages, but a few of them met the necessary requirements such as support for symmetric and asymmetric algorithms or hash operations.

4.2 Expansion measures

The next step of analysis was to select the packages which fulfill the requirements. The relevant parameters were the support of all cryptographic functions, the topicality of project, the approach to solving problems and no payment license. In the table 4.2, there are shown four libraries which are compared to the base of the other measures:

- Generation crypto. key - possibilities for generation of cryptographic keys (Yes/No),
- Key size min. - if package could generate cryptographic key, it shows minimal key size in bytes (some packages do not provide this information),
- Key size max. - if package could generate cryptographic key, it shows maximal key size in bytes (some packages do not provide this information),
- X.509 Certificates - work with X.509 certificates (generation of self-signed certificates, support for certificate signing requests, support for different formats and extensions) (Yes/No),
- SSL/TLS - support of higher level protocols such as SSL/TLS (Yes/No),
- TLS_PSK - support communication with the server by using the pre-shared key (Yes/No).

Based on observed data I decided to use Crypto package created by *Golang* for implementation.

Crypto supports generation cryptographic keys and their size is from 2 to 8192 bytes, as suggests table 1 in [31]. The other important requirement is propped up higher level protocols such as SSL/TLS. Only the Crypto package contains subdirectory worked with TLS connection to the server.

Table 4.2: Filtered table of packages with expansion measures

| Package | crypto | jose | go-libp2p- crypto | go- ethereum |
|----------------------------|--------|--------------|----------------------|-----------------|
| Founder | Golang | SermoDigital | libp2p | ethereum |
| Crypto. functions | all | all | all | all |
| Start of project | 2009 | 2015 | 2015 | 2013 |
| Is still opened | Y | Y | Y | Y |
| Issue tracker system | Y | Y | Y | Y |
| Doc. accessability | 5 | 4 | 4 | 4 |
| Downloads | - | 28 | 5 | 1028 |
| License | Y | Y | Y | Y |
| Generation crypto. keys | Y | N | Y | N |
| Key size min | 2 | - | unknown | - |
| Key size max | 8192 | - | unknown | - |
| X.509 Certificates | Y | Y | Y | Y |
| SSL/TLS | Y | N | N | N |
| TLS_PSK ¹ | N | N | N | N |

¹ During analysis I found package *Raff/tls-psk* using TLS_PSK cipher suites, I describe it in subsection 5.2.1.

5 Implementation

The practical part of my Bachelor thesis is to implement console application to create keys and certificates which are signed by internal certificate authority. In this chapter, I will explain the assignment, the problems and the process of implementation.

5.1 Assignment

For functionality, there are needed several parameters, such as:

- the address of the server with the certificate authority,
- the port connection to the server,
- the pre-shared key to connect to server,
- path to the key store,
- IP address of subsystem,
- the domain name of subsystem and
- identity of a system for what the certificate is created.

The application connects to the server with intern certificate authority through TLS_PSK, then it generates the asymmetric RSA key pair and the certification signing request which is sent to the authority. Server sends signed certificate back and it is along with private key saved to the designated key store.

5.2 TLS_PSK

For application I decided to use packages created by Golang. There was a problem because this package does not support TLS with pre-shared key. From the previous research I know that there is one third-party library which is adapted to use TLS_PSK [32].

5.2.1 Raff

Raff/tls-psk library was created 3 years ago and it has not been maintained yet. It does not have any downloads, issue tracker nor active contributors.

For application needed I decided to try this library. Connecting to *OpenSSL* server was correct but connecting to server with CA was not possible because of unsupported cipher suites. *Raff/tls-psk* library contains only 4 versions of cipher suites and the others are not supported.

To solving the issue, one of the supported cipher suites was added to the test server. It turned out that package *Raff/tls-psk* has also some other issues whose I have not examined yet.

The other solution how to implement TLS_PSK to Go is using Cgo. Cgo allows Go to interoperate code written in C language. How Cgo works I describe in section 3.4.

5.3 Language C in Go

I created methods worked with *OpenSSL* in language C for initialization, connection, reading from and writing to the server.

5.3.1 Initialization

Initialization consists of four methods from *openssl/ssl.h* and *openssl/err.h*. Methods initialize *s_client*, add algorithms to the table and register the error strings, the available SSL/TLS ciphers and digests.

5.3.2 Connection

Connection to the server is created through TLS_PSK. Connection method creates a new SSL_CTX object as a framework to establish TLS/SSL enabled connections, next it creates a new BIO chain consisting of an SSL BIO (using ctx) followed by a setting of address and pre-shared key. The address consists of host name and port. The pre-shared key is set through *SSL_set_psk_client_callback* with SSL and a callback function as arguments. The purpose of the callback function is to select the PSK identity and the pre-shared key to use during the connection setup phase. The variable with the pre-shared key has to be global. The setting is followed by a connect BIO.

5.3.3 Reading from and writing to server

Created method *C_bio_read* reads 1 byte from BIO until the server sends the null terminator `'\0'`. Created method *C_bio_write* writes bytes to BIO with the null terminator `'\0'` at the end.

5.4 Using C-methods in Go

Methods written in C language have to be called in Go code with prefix `'C.'` and have the correct types of arguments.

C does not have an explicit string type and strings are represented by a zero-terminated array of chars. Conversion between Go and C strings is done with the *C.CString*, *C.GoString*, and *C.GoStringN* functions. These conversions make a copy of the string data [17].

```
1 // Go string to C string
2 func C.CString(string) *C.char
3
4 // C string to Go string
5 func C.GoString(*C.char) string
6
7 // C data with explicit length to Go string
8 func C.GoStringN(*C.char, C.int) string
```

As I wrote in the subsection 5.3.2, the pre-shared key has to be the global variable in C code. To set it from Go code where application takes the pre-shared key as an argument, I used followed commands.

```
1 //in C
2 char *psk_key;
3
4 //in Go
5 arg := os.Args
6 private_key := arg[3]
7
8 C.psk_key = C.CString(private_key)
```

5.5 Communication protocol

Communication between the application and server containing the internal Certificate Authority (CA Server) is based on null-terminated strings. The protocol looks as follows:

5.5.1 Connection using TLS_PSK

- The application connects to the CA Server using given pairing key and default identity.
- The CA Server validates the application.

The connection is provided via Go method *create_connection* with arguments port, the address of the server and pre-shared key. The pre-shared key is set as a global variable in C code (described in section 5.4) and subsequently is called C method to create the connection. Pre-shared key has to be a string.

Client and server exchanged *ClientHello* - *ServerHello*, and *ClientKeyExchange* - *ServerKeyExchange*. They agreed to use common cipher suite.

5.5.2 Protocol version exchange

- The application sends supported protocol version.
- The CA Server chooses the highest protocol version possible and sends it back.

Currently is used only protocol version 1. Go method calls writing and reading methods from C code.

```
1 protocol_version := C.CString("1")
2 err_write := C.C_bio_write(bio, protocol_version, 1)
3 server_protocol_version := C.C_bio_read(bio)
4 if *server_protocol_version != *protocol_version {
5     return -1
6 }
```

5.5.3 Key length

- The application sends the component/subsystem identification.
- The application sends information if the key/certificate belongs to the intermediate CA or it is end certificate (CA or END).
- The CA Server returns key length for the key generation.

There are used C methods for write and read. The subsystem identification (UA) is written to the server together with CA or END information from argument of application. Subsequently, the method reads *key_length* from server and uses standard library functions to

convert string to the number from package *"strconv"* and generates the key from package *"crypto/rsa"*.

```
1 key_len, err := strconv.Atoi(C.GoString(key_length))
2 checkErr(err)
3
4 var key interface{}
5 key, err = rsa.GenerateKey(rand.Reader, key_len)
```

5.5.4 Certificate signing

- The application sends generated PEM encoded certificate signing request (with domain name in Common Name field).
- The application sends IP address of the component/subsystem server.
- The CA Server responses with the whole chain signed certificates (PEM encoded).

The application creates the template (tmp) based on observed IP address and domain_name from arguments. The template (tmp) is used during creating a new certificate request (CSR).

```
1 tmp := &x509.CertificateRequest {
2     Subject      : pkix.Name{CommonName : ip},
3     DNSNames     : []string{domain_name},
4     IPAddresses  : []net.IP{net.ParseIP(ip)},
5 }
6 csr, err := x509.CreateCertificateRequest(rand.Reader, tmp, key)
```

The template and function *CreateCertificateRequest* are from package *"crypto/x509"*. The function returns bytes array, so to sending the request to the server, it has to be converted to pem string. The request has to be saved in temp file as follows:

```
1 pem.Encode(csr_file, &pem.Block{Type: "CERTIFICATE REQUEST",
    Bytes: csr})
```

and subsequently, it is read as a string and sent to the server. When the file with request is not needed, it is deleted through:

```
1 os.Remove("csr.pem")
```

The server answers with signed certificate chain. Signed certificate is saved to file and together with generated key they are saved to the key store.

5. IMPLEMENTATION

5.5.5 Achieving trust

The connection ends when the server sends trust anchor as a CA certificate. After that, it is not possible to write to or read from the server. Correctness of achieving trust is checked up through:

```
1 strings.HasPrefix(str, "-----BEGIN")
```

5.6 Compilation and run

To run application, it is needed to install several programs.

1. Go - see how to start with Go in section 3.2
2. GCC - the application use Cgo which needs C compiler
3. OpenSSL - is used in C code
4. libssl-dev - (or openssl-devel) contains compiled dynamic libraries *libssl* and *libcrypto* important for linker options (part of LDFLAGS).
 - (a) *libssl* provides the client and server-side implementations for SSLv3 and TLS.
 - (b) *libcrypto* provides general cryptographic and X.509 support needed by SSL/TLS [33].

Application is built and run through:

```
1 go build <name>.go
2 ./<name> <server> <port> <PSK> <pathToKeyStore> <subjectIP>
  <subjectDomainName> <subjectID>
```

For example:

```
1 go build app.go
2 ./app localhost 10443 aaaa /tmp 192.0.2.0 example.com END
```

6 Evaluation

In this chapter, I will evaluate process of working on this thesis. I will describe the workflow, the problems and way how to integrate the application in the company system.

6.1 Select Libraries

Before analyzing libraries, I had to learn Go language, install it and try to programming. All important information about this language and working with it is described in the chapter 3.

The Internet provides a big amount of Go packages created by third parties. To the thesis, I selected more than one hundred packages working with cryptographic functions and hash operations. It was necessary to remove packages from untrusted and unsupported sources. The correct packages in table 4.1 are compared based on their actuality (topicality), the approach to solving problems, documentation accessibility, number of downloads and no payment license. The table 4.2 contains 4 libraries selected from table 4.1.

The analysis shows that until today, a package that is suitable with all the requirements does not exist. The generation of cryptographic keys (within 2 to 8192 bytes) and support of TLS protocol at the same time is only in package *Crypto* from *Golang*. This is the main reason why i chose it to use it in the implementation although the final application uses *OpenSSL* for the connection.

During the analysis I found package *Raff/tls-psk* using TLS_PSK cipher suites, but the package has not been supported for 3 years, so it was not possible to use this package in the implementation.

The problem with TLS_PSK solves using *OpenSSL*.

6.2 OpenSSL and Language C

OpenSSL contains an open-source implementation of the SSL/TLS protocols. The libraries, written in the C programming language, implements basic cryptographic functions and provides various utility functions [35].

In the implementation was needed to create methods working with *OpenSSL* in language C. The methods are described in section 5.3 and called from Go code using Cgo (explained in section 3.4). The whole implementation is divided into the functions and strictly adheres communication protocol (see section 5.5).

The application requires installing package *libssl-dev* (or *openssl-devel* on Fedora). This package is part of the *OpenSSL* project's implementation of the SSL and TLS cryptographic protocols for secure communication over the Internet. It contains development libraries, header files, and manpages for *libssl* and *libcrypto*. `LD_FLAGS` and `C_FLAGS` are defined with pseudo `#cgo` directives within comments to tweak the behavior of the C compiler.

```
1 #cgo CFLAGS: -Iaddress/to/openssl/include
2 #cgo LDFLAGS: -lcrypto -lssl
```

During the implementation did not rise any other problem.

6.3 Testing

The necessary step of implementation is testing multiple parts of application and all of the system acting together. I test whether each component fulfills its contract, but also whether they are composed and configured correctly and interact as expected.

6.3.1 Connectivity test

Connectivity test checks behavior of application for the wrong server, port or key. For the wrong server or port, the application returns *BIO_do_connect*: -1 what means the connection failed. For the wrong key, the application writes checking identity and key, *BIO_do_connect*: -1 what means that the connection failed for the wrong key.

6.3.2 Step by step testing of communication

I created tests for checking communication in certain moments. Each test has to contain connection and the previous steps of communication to correct test of given step.

For example test of protocol version exchange contains the correct connection to the server.

```
1 func Test_version_exchange_OK(t *testing.T) {  
2     t.Log("Testing protocol version exchange... ")  
3  
4     bio := create_connection("localhost", "10443", "aaaa")  
5     if bio == nil {  
6         t.Errorf("Error while connecting to server")  
7     }  
8  
9     if ret := protocol_version_exchange(bio); ret == -1 {  
10        t.Errorf("Error: different version")  
11    } else if ret == -2 {  
12        t.Errorf("Error: problem with connection")  
13    }  
14    t.Log("Test OK")  
15 }
```

Tests of generation certificate request and private key also contain generation with the correct and wrong connection, arguments and key size.

6.3.3 File test

These tests check saving certificates and keys without connection and previous communication with the server to the key store with the existing or non-existing path, correct key or empty interface.

7 Conclusion

This Bachelor thesis deals with cryptographic tools of Go programming language. The aim was to evaluate Go cryptographic libraries and implement the prototype of a client application able to generate asymmetric keys and certificate signing requests and connect to a server application using TLS_PSK cipher suite. The thesis was consulted and realized in cooperation with Y Soft Corporation, a.s.

The Go libraries were overviewed and compared based on their support of symmetric and asymmetric cryptographic algorithms and hash operations. In pursuance of analysis, the four libraries were selected and subsequently examined according to methods for generation of cryptographic keys and self-signed certificates, support for certificate signing requests, different formats, and SSL/TLS. From the report, one library was selected for the implementation.

The prototype of a client application is implemented in language Go which interoperates with methods in language C. The source code contains the both languages written according to rules of Cgo. C methods serve the connection to the server and the communication between the client and the server using OpenSSL. Go methods serve subjects of communication concretely. During implementation, I solved problems with non-supported library and OpenSSL integration. The client's application is prepared to integrate to the company system.

The Bachelor thesis had a great personal benefit for me. I expanded my knowledge of Go programming language, OpenSSL, and the certificates. I also gain a great asset in designing and developing the application and I improved my programming skills in the languages C and Go.

Bibliography

1. DOSTÁLEK, Libor; VOHNOUTOVÁ, Marta. *Velký průvodce infrastrukturou PKI*. Computer Press, Albatros Media as, 2016.
2. SCHMEH, Klaus. *Cryptography and public key infrastructure on the Internet*. John Wiley & Sons, 2006.
3. SINGH, Simon; KOUBSKÝ, Petr; ECKHARDTOVÁ, Dita. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. Dokořán, 2003.
4. HOW TO SSL. *PEM Files*. 2017. Available also from: http://how2ssl.com/articles/working_with_pem_files/. [Online; 21-02-2017].
5. BAKKER, Paul. *ASN.1 key structures in DER and PEM*. 2014. Available also from: <https://tls.mbed.org/kb/cryptography/asn1-key-structures-in-der-and-pem>. [Online; 21-02-2017].
6. OPPLIGER, Rolf. *Security technologies for the world wide web*. Artech House, 2003.
7. FREIER, Alan; KARLTON, Philip; KOCHER, Paul. *The secure sockets layer (SSL) protocol version 3.0*. 2011. Technical report.
8. RESCORLA, E. *The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-20*. 2017. Technical report.
9. CASWELL, Matt. *Using TLS1.3 With OpenSSL*. 2017. Available also from: <https://www.openssl.org/blog/blog/2017/05/04/tls1.3/>. [Online; 05-05-2017].
10. MICROSOFT. *TLS Handshake Protocol*. 2017. Available also from: [https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513(v=vs.85).aspx). [Online; 08-05-2017].
11. TAUBERT, Tim. *More Privacy, Less Latency*. 2015. Available also from: <https://timtaubert.de/images/tls13-hs-resumption.png>. [Online; 10-05-2017].
12. ERONEN, Pasi; TSCHOFENIG, Hannes. *Pre-shared key ciphersuites for transport layer security (TLS)*. 2005. Technical report.
13. DOXSEY, Caleb. *Introducing Go*. O'Reilly Media, 2016.

BIBLIOGRAPHY

14. HARA, Mikio. *golang/go*. 2017. Available also from: <https://github.com/golang/go/wiki>. [Online; 27-02-2017].
15. VARGHESE, Shiju. *Understanding Golang Packages*. 2014. Available also from: <https://thenewstack.io/understanding-golang-packages/>. [Online; 27-02-2017].
16. GOLANG. *Command cgo*. 2017. Available also from: <https://golang.org/cmd/cgo/>. [Online; 24-03-2017].
17. GERRAND, Andrew. *The Go Blog*. 2011. Available also from: <https://blog.golang.org/c-go-cgo>. [Online; 25-03-2017].
18. DOGAN, Jaana Burcu. *golang/go*. 2016. Available also from: <https://github.com/golang/go/wiki/cgo>. [Online; 25-03-2017].
19. CHISNALL, David. *The Go programming language phrasebook*. Addison-Wesley, 2012.
20. HARRIS, Alan. *Go: Up and Running*. O'Reilly Media, 2015.
21. KOZYRA, Nathan. *Mastering concurrency in go*. Packt Publishing, 2014.
22. GOLANGLIBS. *Security*. 2017. Available also from: <https://golanglibs.com/top?q=security>. [Online; 27-02-2017].
23. GOLANGLIBS. *Cryptography - Go libraries and apps*. 2017. Available also from: <https://golanglibs.com/category/cryptography?sort=top>. [Online; 27-02-2017].
24. GO DOC. *crypto - GoDoc*. 2017. Available also from: <https://godoc.org/golang.org/x/crypto>. [Online; 27-02-2017].
25. GOLANG. *Packages*. 2017. Available also from: <https://golang.org/pkg/>. [Online; 27-02-2017].
26. PURE-GO-LIBS. *Pure Go Libs*. 2017. Available also from: <http://golang.cat-v.org/pure-go-lib>. [Online; 27-02-2017].
27. GOLANG. *Package crypto*. 2012. Available also from: <https://golang.org/pkg/crypto/>. [Online; 18-11-2016].
28. SERMODIGITAL. *SermoDigital/jose*. 2015. Available also from: <https://github.com/SermoDigital/jose>. [Online; 18-11-2016].
29. LIBP2P. *libp2p/go-libp2p-crypto*. 2015. Available also from: <https://github.com/libp2p/go-libp2p-crypto>. [Online; 18-11-2016].

BIBLIOGRAPHY

30. ETHEREUM. *ethereum/go-ethereum*. 2013. Available also from: <https://github.com/ethereum/go-ethereum>. [Online; 18-11-2016].
31. HINEK, Jason. On the security of multi-prime RSA. *Journal of Mathematical Cryptology*. 2008, vol. 2, no. 2, pp. 117–147.
32. RAFF. *raff/tls-psk*. 2014. Available also from: <https://github.com/raff/tls-psk>. [Online; 27-02-2017].
33. OPENSSL. *openssl/openssl*. 2016. Available also from: <https://github.com/openssl/openssl>. [Online; 02-05-2017].
34. DIE.NET. *Section 3: library functions - Linux man pages*. 2017. Available also from: <https://linux.die.net/man/3/>. [Online; 02-05-2017].
35. FOUNDATION, Inc. OpenSSL. *Manpages for 1.0.2*. 2017. Available also from: <https://www.openssl.org/docs/man1.0.2/>. [Online; 02-05-2017].