

The OpenSSL Guide

The OpenSSL Project

January 29, 2018

Contents

I	Foundations	2
1	Outline - to be deleted	3
2	About OpenSSL	8
II	SSL/TLS/DTLS	9
III	Cryptography	10

Part I

Foundations

Chapter 1

Outline - to be deleted

I. Part: Foundations

A. Chapter: Introduction

1. Purpose of this book
2. Layout and how to navigate this book
3. This is an open source book
4. About the authors

B. Chapter: About OpenSSL

1. What is OpenSSL
 - a. Describe OpenSSL as a command line tool
 - b. Describe OpenSSL as a SSL/TLS/DTLS library
 - c. Describe OpenSSL as a crypto library
2. OpenSSL History
 - a. SSLeay
 - b. OpenSSL formation
 - c. The lean years and FIPS
 - d. Changes in the team membership and processes
 - e. OpenSSL today

C. Chapter: Getting OpenSSL

1. OpenSSL Version Numbering
2. Using pre-built binaries
3. Pre-requisites for building OpenSSL from source
4. Compiling and installing from source
5. Troubleshooting some common build issues

D. Chapter: Programming Fundamentals

1. Memory management
 - a. new and free functions

- b. OPENSSL_malloc, OPENSSL_zalloc and OPENSSL_free
 - c. get0, get1, set0, set1 etc
 - d. Debugging memory issues
 - 2. BIOs
 - 3. Serialisation and De-serialisation
 - a. i2d and d2i functions
 - 4. Stacks
 - 5. LHashes
 - 6. NIDs
 - 7. Identifying the OpenSSL version
 - 8. Automatic Library Initialisation and De-initialisation
 - 9. Threads
- E. Chapter: Certificates and Certificate Authorities
- F. Chapter: Working with Certificate and Key files
- 1. PEM files
 - 2. PKCS8 files
 - 3. PCKS12 files
- G. Chapter: Certificate Revocation
- 1. CRLs
 - 2. OCSP
- H. Chapter: Configuration via CONF
- I. Chapter: Engines (Advanced Topic)
- J. Chapter: Stores (Advanced Topic)
- K. Chapter: Advanced Certificates (Advanced Topic)
- L. Chapter: Certificate Transparency (Advanced Topic)
- M. Chapter: Asynchronous operation (Advanced Topic)
- N. Chapter: ASN.1 (Advanced Topic)
- O. Chapter: UIs (Advanced Topic)
- II. Part: SSL/TLS/DTLS
- A. Chapter: Understanding SSL/TLS
- 1. Security properties of an SSL/TLS connection
 - 2. Overview of SSL/TLS versions
 - 3. Overview of establishing identity
 - 4. Overview of ciphersuites
 - 5. Records
 - 6. Overview of the Handshake
 - 7. Sessions and resumption

B. Chapter: Getting Started

1. Creating an SSL_CTX
2. Creating a self-signed certificate
3. Starting the test server
4. A simple client
 - a. Connecting
 - b. Exchanging data
 - c. Shutting down
5. Compilation
6. Running the client
7. Adding the trusted CAs
8. A simple server
 - a. Setting up the SSL_CTX
 - b. Accepting incoming connections

C. Chapter: Ciphersuites

1. Parts of the Ciphersuite
2. Ciphersuite Naming
3. TLSv1.3 Ciphersuites
4. Configuring the available Ciphersuites
5. Ciphersuite selection (client vs server preference)
6. Key Exchange Mechanisms
 - a. RSA
 - b. DHE
 - c. ECDHE (covering some basics of curve types: P-256, X25519 etc)
 - d. SRP
 - e. PSK
7. Authentication
 - a. RSA
 - b. ECDSA
 - c. EdDSA? (future)
8. Encryption
 - a. AES
 - b. Camellia
 - c. ChaCha
 - d. etc
9. MAC/AEAD

D. Chapter: Basic Operation

1. The read and write BIOs

2. Alerts
 3. Version Negotiation
 4. SSL_read, SSL_write and SSL_get_error
 - a. Non-blocking IO
 - b. Pending data
 5. Shutting down
 6. Client Authentication
 7. Renegotiation
 8. Compression
 9. SSL BIO
 10. Exporting secrets
- E. Chapter: Sessions
1. Resumption handshakes
 2. Simple sessions and session files
 3. Session tickets
 4. Session caches
- F. Chapter: Configuration
1. Setting options and modes
 - a. Some common options/modes
 - (1) SSL_MODE_AUTO_RETRY
 - (2) SSL_MODE_RELEASE_BUFFERS
 2. Signature Algorithms
 3. Supported Groups
 4. Configuration using SSL_CONF
 5. Security levels and the security callbacks
- G. Chapter: DTLS
1. Key differences with TLS
 2. Transports
 - a. UDP
 - b. SCTP
 - c. MTU issues
 3. Retransmissions and the DTLS timer
 4. Listening for connections and cookies
- H. Chapter: TLSv1.3
- I. Chapter: Debugging Connection Failures
- J. Chapter: Advanced Extensions (Advanced Topic)
1. SNI
 2. ALPN and NPN

3. SRTP
 4. EC point formats
 5. Extended Master Secret
 6. Encrypt-Then-MAC
 7. OCSP in SSL/TLS
 8. Certificate Transparency in SSL/TLS
 9. Custom extensions
 - K. Chapter: DANE (Advanced Topic)
 - L. Chapter: Optimisation (Advanced Topic)
 1. Multiblock
 2. Async
 3. Pipelining
 4. Fragment sizes
 5. Read ahead
- III. Part: Cryptography
- A. Chapter: Working with BIGNUMs
 - B. Chapter: Random Numbers
 - C. Chapter: Encryption and Decryption (Symmetric)
 1. What is symmetric encryption
 2. Block and stream ciphers
 3. Modes
 4. IVs and Nonces
 5. A simple encryption/decryption example
 6. AEAD
 - a. Tags
 - b. GCM
 - c. OCB
 - d. CCM
 - e. ChaCha20-Poly1305
 7. XTS
 - D. Chapter: Asymmetric encryption and decryption
 - E. Chapter: Digital signatures
 - F. Chapter: Hashes
 - G. Chapter: Message Authentication Codes
 - H. Chapter: Key Generation and Derivation
 - I. Chapter: CMS (PKCS.7) and S/MIME (Advanced Topic)
 - J. Chapter: Elliptic Curves (Advanced Topic)

Chapter 2

About OpenSSL

[TODO:Add some text here.]

Part II
SSL/TLS/DTLS

Part III

Cryptography