
fastd Documentation

Release 15

Matthias Schiffer

November 11, 2014

1	User manual	1
1.1	Command line options	1
1.2	Configuration file format	2
1.3	Encryption & authentication methods	9
1.4	MTU configuration	11
2	Release notes	13
2.1	fastd v15	13
3	Cryptographic algorithms	15
3.1	ec25519	15
3.2	FHMQV-C	17
3.3	Ciphers	19
3.4	Message Authentication Codes	20
3.5	Method providers	20
4	Developer documentation	23
4.1	Protocol specification	23
	Bibliography	27

1.1 Command line options

Command line options and config files are parsed in order they are specified, so config files specified before other options are overwritten by the other options, config files specified later will overwrite options specified before.

- help, -h** Shows this help text
- version, -v** Shows the fastd version
- daemon, -d** Runs fastd in the background
- pid-file <filename>** Writes fastd's PID to the specified file.
- log-level <error|warn|info|verbose|debug|debug2>** Sets the stderr log level; default is info, if no alternative log destination is configured. If logging to syslog or files is enabled, the default is not to log to stderr.
- syslog-level <error|warn|info|verbose|debug|debug2>** Sets the log level for syslog output; default is not to use syslog.
- syslog-ident <ident>** Sets the syslog identification; default is 'fastd'.
- config, -c <filename>** Loads a config file. - can be specified to read a config file from stdin.
- config-peer <filename>** Loads a config file for a single peer. The filename will be used as the peer name.
- config-peer-dir <dir>** Loads all files from a directory as peer configs. On SIGHUP fastd will reload peer directories.
- mode, -m <tap|tun>** Sets the mode of the interface; default is TAP mode.
- interface, -i <name>** Sets the name of the TUN/TAP interface to use. If not specified, default names specified by the system will be used.
- mtu, -M <mtu>** Sets the MTU; must be at least 576. You should read MTU configuration, the default 1500 is suboptimal in most setups.
- bind, -b <address:port>** Sets the bind address. Address can be an IPv4 address or an IPv6 address, or the keyword any. IPv6 addresses must be put in square brackets.

Default is to bind to a random port, for IPv4 and IPv6. You can specify one IPv4 and one IPv6 bind address, or both at once as any. It is currently not possible to specify an IPv6 link-local address on the command line.

- protocol, -p <protocol>** Sets the handshake protocol. Currently the only protocol available is `ec25519-fhmqvc`, which provides a secure authentication of peers based on public/secret keys.
- method <method>** Sets the encryption/authentication method. See the page [Encryption & authentication methods](#) for more information about the supported methods. More than one method can be specified; the earlier you specify a method the higher is the preference for a method, so methods specified later will only be used if a peer doesn't support the first methods.
- forward** Enables forwarding of packets between clients; read the paragraph about this option before use!
- on-pre-up <command>** Sets a shell command to execute before interface creation. See the detailed documentation below for an overview of the available environment variables.
- on-up <command>** Sets a shell command to execute after interface creation. See the detailed documentation below for an overview of the available environment variables.
- on-down <command>** Sets a shell command to execute before interface destruction. See the detailed documentation below for an overview of the available environment variables.
- on-post-down <command>** Sets a shell command to execute after interface destruction. See the detailed documentation below for an overview of the available environment variables.
- on-connect <command>** Sets a shell command to execute when a handshake is sent to establish a new connection.
- on-establish <command>** Sets a shell command to execute when a new connection is established. See the detailed documentation below for an overview of the available environment variables.
- on-disestablish <command>** Sets a shell command to execute when a connection is lost. See the detailed documentation below for an overview of the available environment variables.
- on-verify <command>** Sets a shell command to execute to check a connection attempt by an unknown peer. See the detailed documentation below for more information and an overview of the available environment variables.
- verify-config** Checks the configuration and exits.
- generate-key** Generates a new keypair.
- show-key** Shows the public key corresponding to the configured secret.
- machine-readable** Suppresses output of explaining text in the `--show-key` and `--generate-key` commands.

1.2 Configuration file format

1.2.1 Main configuration

Example config:

```
# Log warnings and errors to stderr
log level warn;
```

```
# Log everything to syslog
log to syslog level debug;

# Set the interface name
interface "mesh-vpn";

# Support salsa2012+umac and null methods, prefer salsa2012+umac
method "salsa2012+umac";
method "null";

# Bind to a fixed port, IPv4 only
bind 0.0.0.0:10000;

# Secret key generated by `fastd --generate-key`
secret "78dfb05fe0aa586fb017de566b0d21398ac64032fcf1c765855f4d538cc5a357";

# Set the interface MTU for TAP mode with xsalsa20/aes128 over IPv4 with a base MTU of 1492 (PPPoE)
# (see MTU selection documentation)
mtu 1426;

# Include peers from the directory 'peers'
include peers from "peers";

bind <IPv4 address>:<port> [ interface "<interface>" ] [ default [ ipv4 ] ];
bind <IPv6 address>:<port> [ interface "<interface>" ] [ default [ ipv6 ] ];
bind any:<port> [ interface "<interface>" ] [ default [ ipv4|ipv6 ] ];
bind <IPv4 address> port <port> [ interface "<interface>" ] [ default [ ipv4 ]
];
bind <IPv6 address> port <port> [ interface "<interface>" ] [ default [ ipv6 ]
];
bind any port <port> [ interface "<interface>" ] [ default [ ipv4|ipv6 ] ];
```

Sets the bind address, port and possibly interface. May be specified multiple times. The keyword `any` makes fastd bind to the unspecified address for both IPv4 and IPv6. When no bind address is configured at all, for each outgoing connection a new socket with a random port is created.

IPv6 address must be put in square brackets. It is possible to specify an IPv6 link-local address with an interface in the usual notation (e.g. `[fe80::1%eth0]`).

The default option makes it the default address for outgoing connections for IPv4, IPv6 or both.

```
cipher "<cipher>" use "<implementation>";
```

Chooses a specific implementation for a cipher. Normally, the default setting is already the best choice. Note that specific implementations may be unavailable on some platforms or disabled during compilation. The available ciphers and implementations are:

- `aes128-ctr`: AES128 in counter mode
 - `openssl`: Use implementation from OpenSSL's libcrypto
 - `nacl`: Use implementation from NaCl or libsodium
- `null`: No encryption (for authenticated-only methods using `composed_gmac`)

- memcpy: Simple memcpy-based implementation
- salsa20: The Salsa20 stream cipher
 - xmm: Optimized implementation for x86/amd64 CPUs with SSE2 support
 - nacl: Use implementation from NaCl or libsodium
- salsa2012: The Salsa20/12 stream cipher
 - xmm: Optimized implementation for x86/amd64 CPUs with SSE2 support
 - nacl: Use implementation from NaCl or libsodium

```
drop capabilities yes|no|early;
```

By default, fastd switches to the configured user and/or drops its POSIX capabilities after the on up command has been run. When drop capabilities is set to early, the on up command is run after the privileges have been dropped, when set to no, the POSIX capabilities aren't dropped at all (but the user is switched after the on up command has been run nevertheless).

```
forward yes|no;
```

Enables or disabled forwarding packets between peers. Care must be taken not to create forwarding loops.

```
group "<group>";
```

Sets the group to run fastd as.

```
hide ip addresses yes|no;
```

Hides IP addresses in log output.

```
hide mac addresses yes|no;
```

Hides MAC addresses in log output.

```
include "<file>";
```

Includes another configuration file. Relative paths are interpreted relatively to the including file.

```
include peer "<file>" [ as "<name>" ];
```

Includes a peer configuration (and optionally gives the peer a name).


```
include peers from "<dir>;"
```

Includes each file in a directory as a peer configuration. These peers are reloaded when fastd receives a SIGHUP signal.

```
interface "<name>;"
```

Sets the name of the TUN/TAP interface to use; it will be set by the OS when no name is configured explicitly.

```
log level fatal|error|warn|info|verbose|debug|debug2;
```

Sets the default log level, meaning syslog if there is currently a level set for syslog, and stderr otherwise.

```
log to stderr level fatal|error|warn|info|verbose|debug|debug2;
```

Sets the stderr log level. By default no log messages are printed on stderr, unless no other log destination is configured, which causes fastd to log to stderr with level info.

```
log to syslog [ as "<ident>" ] [ level  
fatal|error|warn|info|verbose|debug|debug2 ];
```

Sets the syslog log level. By default syslog isn't used.

```
mac "<MAC>" use "<implementation>;"
```

Chooses a specific implementation for a message authentication code. Normally, the default setting is already the best choice. Note that specific implementations may be unavailable on some platforms or disabled during compilation. The available MACs and implementations are:

- ghash: The MAC used by the GCM and GMAC methods
 - pclmulqdq: An optimized implementation for modern x86/amd64 CPUs supporting the PCLMULQDQ instruction
 - builtin: A generic implementation
- uhash: The MAC used by the UMAC methods
 - builtin: A generic implementation

```
method "<method>;"
```

Sets the encryption/authentication method. See the page [Encryption & authentication methods](#) for more information about the supported methods. When multiple method statements are given, the first one has the highest preference.

```
mode tap|tun;
```

Sets the mode of the interface; the default is TAP mode.

```
mtu <MTU>;
```

Sets the MTU; must be at least 576. You should read the page [MTU configuration](#) as the default 1500 is suboptimal in most setups.

```
on pre-up [ sync | async ] "<command>";
on up [ sync | async ] "<command>";
on down [ sync | async ] "<command>";
on post-down [ sync | async ] "<command>";
on connect [ sync | async ] "<command>";
on establish [ sync | async ] "<command>";
on disestablish [ sync | async ] "<command>";
```

Configures a shell command that is run after the interface is created, before the interface is destroyed, when a handshake is sent to make a new connection, when a new peer connection has been established, or after a peer connection has been lost. fastd will block until the command has finished, to long-running processes should be started in the background.

pre-up, up, down and post-down commands are executed synchronously by default, meaning fastd will block until the commands have finished, while the other commands are executed asynchronously by default. This can be changed using the keywords sync and async.

The following environment variables are set by fastd for all commands:

- FASTD_PID: fastd's PID
- INTERFACE: the interface name
- INTERFACE_MTU: the configured MTU
- LOCAL_KEY: the local public key

For on connect, on establish and on disestablish the following variables are set in addition:

- LOCAL_ADDRESS: the local IP address
- LOCAL_PORT: the local UDP port
- PEER_ADDRESS: the peer's IP address
- PEER_PORT: the peer's UDP port
- PEER_NAME: the peer's name in the local configuration
- PEER_KEY: the peer's public key

```
on verify [ sync | async ] "<command>";
```

Configures a shell command that is run on connection attempts by unknown peers. The same environment variables as in the `on establish` command are supplied. When the command returns 0, the connection is accepted, otherwise the handshake is ignored. By default, fastd ignores connections from unknown peers.

Verify commands are executed asynchronously by default. This can be changed using the keywords `sync` and `async`.

```
packet mark <mark>;
```

Defines a packet mark to set on fastd's packets, which can be used in an ip rule.

Marks can be specified in decimal, hexadecimal (with a leading 0x), and octal (with a leading 0).

```
peer "<name>" { peer configuration }
```

An inline peer configuration.

```
peer group "<name>" { configuration }
```

Configures a peer group.

```
peer limit <limit>;
```

Sets the maximum number of connections for the current peer group.

```
pmtu yes|no|auto;
```

Enables or disables Path MTU detection for IPv4. If enabled, all packets are sent with DF set, and all fragmentation happens on the sending host itself. If disabled, routers may fragment the packets themselves, possibly leading to multiple fragmentation. In general, disabling this should not be necessary, but in some networks ICMP MTU Too Big packets are lost, so PMTU detection doesn't work correctly.

If possible, fastd's mtu setting should be adjusted so the packets aren't fragmented at all instead of relying on this option.

The default is `auto`, which uses the system default as specified in `/proc/sys/net/ipv4/ip_no_pmtu_disc`.

The `pmtu` option is available on Linux platforms only.

```
protocol "<protocol>;"
```

Sets the handshake protocol; at the moment only `ec25519-fhmqvc` is supported.

```
secret "<secret>;"
```

Sets the secret key.

```
secure handshakes yes|no;
```

fastd v11+ implements a revised handshake scheme which prevents downgrade attacks (i.e. an attacker forcing two peers to use the least secure encryption method supported by both sides, or even half-establishing a session with an encryption method supported by one side only). To maintain backwards compatibility, the old handshake is still supported when secure handshakes is set to no.

Setting this option to yes (the default) on one side is enough to ensure that a session established by two peers has not been downgraded.

```
user "<user>;
```

Sets the user to run fastd as.

1.2.2 Peer configuration

Example config:

```
key "f05c6f62337d291e34f50897d89b02ae43a6a2476e2969d1c8e8104fd11c1873";
remote 192.0.2.1:10000;
remote [2001:db8::1]:10000;
remote ipv4 "fastd.example.com" port 10000;
```

```
include "<file>;
```

Includes another configuration file.

```
key "<key>;
```

Sets the peer's public key.

```
remote <IPv4 address>:<port>;
remote <IPv6 address>:<port>;
remote [ ipv4|ipv6 ] "<hostname>":<port>;
remote <IPv4 address> port <port>;
remote <IPv6 address> port <port>;
remote [ ipv4|ipv6 ] "<hostname>" port <port>;
```

Sets the IP address or host name to connect to. If a peer doesn't have a remote address configured, incoming connections are accepted, but no own connection attempts will be made.

The ipv4 or ipv6 options can be used to force fastd to resolve the host name for the specified protocol version only.

Starting with fastd v9, multiple remotes may be given for a single peer. If this is the case, they will be tried one after another. Starting with fastd v11, all addresses a given hostname resolves to are taken into

account, not only the first one. This can be use to specify alternative hostname, addresses and/or ports for the same host; all remotes must still refer to the same peer as the public key must be unique.

```
float yes|no;
```

The float option can be used to accept connections from the peer with the specified key from other addresses that the configured ones.

1.3 Encryption & authentication methods

fastd supports various combinations of ciphers and authentication schemes using different method providers. All ciphers, message authentication codes (MACs) and method providers can be disabled during compilation to reduce the binary size.

See [Benchmarks](#) for an overview of the performance of the different methods.

1.3.1 Recommended methods

The method `salsa2012+umac` is recommended for authenticated encryption. `null+salsa2012+umac` is the recommended method for authenticated-only operation.

Salsa20/12 is a stream cipher with very high speed and a very comfortable security margin. It has been chosed for the software profile in the [eSTREAM](#) project in 2008.

[UMAC](#) is an extremely fast message authentication code which is provably secure and optimized for software implementations.

OpenWrt

Too keep the binary as small as possible, only the following methods are enabled on OpenWrt by default:

- `salsa2012+gmac`
- `salsa2012+umac`
- `null+salsa2012+gmac`
- `null+salsa2012+umac`
- `null`

Of these, the GMAC-based methods may be dropped in the future to further reduce the binary size, as UMAC is the superior authentication scheme (it is faster than GMAC, provably secure and its software implementation isn't suspect to timing side channels).

1.3.2 List of methods

Encrypted methods

Method	Method provider	Cipher	MAC	Notes
aes128-gcm	generic-gmac	aes128-ctr	ghash	⁴
salsa20+gmac	generic-gmac	salsa20	ghash	
salsa2012+gmac	generic-gmac	salsa2012	ghash	
aes128-ctr+umac	generic-umac	aes128-ctr	uhash	²
salsa20+umac	generic-umac	salsa20	uhash	
salsa2012+umac	generic-umac	salsa2012	uhash	
aes128-ctr+poly1305	generic-poly1305	aes128-ctr	none ⁵	^{2, 6}
salsa20+poly1305	generic-poly1305	salsa20	none ¹	³
salsa2012+poly1305	generic-poly1305	salsa2012	none ¹	³

This list is not exhaustive. It is possible to combine different ciphers for data and authentication tag encryption using the *composed-gmac* and *composed-umac* method providers; these methods aren't listed here as this is not very useful.

Authenticated-only methods

Method	Method provider	Cipher	MAC	Notes
null+aes128-gmac	composed-gmac	aes128-ctr	ghash	^{2, 8}
null+salsa20+gmac	composed-gmac	salsa20	ghash	⁴
null+salsa2012+gmac	composed-gmac	salsa2012	ghash	⁴
null+aes128-ctr+umac	composed-umac	aes128-ctr	uhash	^{2, 4}
null+salsa20+umac	composed-umac	salsa20	uhash	⁴
null+salsa2012+umac	composed-umac	salsa2012	uhash	⁴

Methods without security

Method	Method provider	Cipher	MAC	Notes
null	null	none	none	¹⁰

Deprecated methods

Method	Method provider	Cipher	MAC	Notes
xsalsa20-poly1305	xsalsa20-poly1305	none	none	¹²

Since fastd v11 `salsa20+poly1305` should be used instead (or even better a more performant method like `salsa2012+gmac`); `xsalsa20-poly1305` will be removed eventually.

¹AES is very slow without OpenSSL support. OpenSSL's AES implementation may be suspect to cache timing side channels when no hardware support like AES-NI is available.

²The MAC is integrated in the method provider.

³Poly1305 is very slow on embedded systems.

⁴AES is very slow without OpenSSL support. OpenSSL's AES implementation may be suspect to cache timing side channels when no hardware support like AES-NI is available.

⁵The MAC is integrated in the method provider.

⁶Poly1305 is very slow on embedded systems.

⁷The cipher is used to encrypt the authentication tag only, the actual data is transmitted unencrypted.

⁸The cipher is used to encrypt the authentication tag only, the actual data is transmitted unencrypted.

⁹Only authentication of peers' IP addresses, but no encryption or authentication of any data is provided.

¹⁰Only authentication of peers' IP addresses, but no encryption or authentication of any data is provided.

¹¹Both the cipher and the MAC are integrated in the method provider.

¹²Both the cipher and the MAC are integrated in the method provider.

1.4 MTU configuration

The default MTU of fastd is 1500. This allows bridging the fastd interface in TAP mode with other interface with the same MTU, but will usually cause fastd's UDP packets to be fragmented (see also the option *pmtu*). Fragmentation can lower the performance or even cause connectivity problems when broken routers filter ICMP packets, so if possible the MTU should be chosen small enough so that IP fragmentation can be avoided. Unlike OpenVPN, fastd doesn't support fragmentation itself, but relies on the IP stack to fragment packets when necessary.

1.4.1 Guidelines

- The basic overhead of a fastd packet in TUN mode over IPv4 is 39 Bytes when only null crypto is used and 52 Bytes for all other crypto methods
- TAP mode needs 14 bytes more than TUN mode
- Tunneling over IPv6 needs 20 bytes more than IPv4

1.4.2 Examples

Your base MTU is 1500 and you want to use TUN mode over IPv4 with any crypto method: Choose $1500 - 52 = 1448$ bytes.

Your base MTU is 1492 (like most German DSL lines) and you want to use TAP mode over IPv4 with any crypto method: Choose $1492 - 52 - 14 = 1426$ bytes.

Conservative choice when you want to transfer IPv6 inside the tunnel: Choose 1280 Bytes (not relevant when you use batman-adv inside the tunnel as batman-adv will take care of the inner fragmentation).

Conservative choice when you don't know anything (but assume the base MTU is at least 1280 so IPv6 can be supported) and w
Choose $1280 - 52 - 14 - 20 = 1194$ bytes.

Release notes

2.1 fastd v15

2.1.1 New features

- New message authentication code UMAC

The new message authentication code UMAC provides very high security with much higher performance than the old GMAC methods. “salsa2012+umac” and “null+salsa2012+umac” are the new recommended methods for authenticated encryption and authenticated-only operation.

- Status socket

A unix socket can be configured with the new *status socket* option. fastd will dump its current state as JSON on every connection on this socket; this status output is much more detailed than the old SIGUSR1 output. SIGUSR1 is ignored now.

To compile fastd with status socket support, libjson-c is required. An example script to get the status can be found at `doc/examples/status.pl`.

- MacOS X support

fastd should now also run on recent versions of MacOS X. The unofficial TUN/TAP driver is required for this.

- New Sphinx-based documentation
- Fix warnings with CMake 3.0
- OpenWrt: allow setting on-connect, on-verify, on-establish... hooks via UCI
- OpenWrt: allow specifying bind interfaces in UCI

2.1.2 Bugfixes

- Signal handling improvements

This should fix an issue where asynchronous handler scripts would be left as zombie processes occasionally.

- Config check fixes in TUN mode

For some configuration mistakes, fastd would segfault instead of printing an error message.

2.1.3 Other changes

- Nicer error messages for common configuration mismatches like having no common methods
- When no port is given in a *bind* directive, a new random port will be chosen now for every new connection attempt (like it was already done when no bind address was configured at all)

This allows setting additional bind options like interface binds without setting a static port.

- The peer hashtable is now grown dynamically to reduce memory usage for small numbers of peers and improve performance for huge numbers of peers
- Major refactoring: the internal peer and peer config structs have been merged
- Internally, int64 timestamps in milliseconds are now used always instead of struct timespec

Milliseconds resolution and int64 range is completely sufficient, and many parts of the code have become simpler due to this change.

Cryptographic algorithms

3.1 ec25519

3.1.1 Twisted Edwards curves

In general, a twisted Edwards curve is a mathematical group on the points satisfying an equation of the form

$$ax^2 + y^2 = 1 + dx^2y^2$$

For purposes of cryptography the curve is defined on a finite field.

The corresponding group law is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

For further information on twisted Edwards curves see [BBJ+08].

Extended coordinate representation

Representing a curve point as an coordinate pair (x, y) is rather inconvenient for calculations on points as reciprocation is a very expensive operation. [HWCD08] specifies an alternative representation: the *extended coordinate* representation, which stores a point as a tuple of four coordinates X, Y, Z and T , satisfying the following equations:

$$x = \frac{X}{Z} \quad y = \frac{Y}{Z} \quad x \cdot y = \frac{T}{Z}$$

By storing the denominator of the fractions as Z , consequent group operations can be performed without having to compute reciprocals until a canonical representation is needed again. The additional value T is used to speed up some operations.

The extended coordinate representation of twisted Edwards curves allows very efficient *strongly unified addition*; the term *strongly unified addition* denotes that the implementation of the addition operation can be used to double a point as well, so the special case of adding a point to itself doesn't have to be implemented specifically.

As the data of the Explicit-Formulas Database [EFD] suggests, the extended coordinate representation of twisted Edwards curves allows strongly unified addition with the least number of operations of all similar curve types and representations in the database (i. e. 9 multiplications), which is the principal reason a twisted Edwards curve has been chosen for fastd's handshake.

Point compression

As the points of an elliptic curve satisfy a curve equation, it is possible to transform the coordinates of a point into a more compact representation for transmission or storage. The twisted Edwards curve equation can be transformed to:

$$y^2 = \frac{1 - ax^2}{1 - dx^2}$$

As one can easily see, there are at most two possible y values for each value of x (this rule also holds when the elliptic curve is defined over a finite field), thus one bit is enough to distinguish between the two values.

For the curve used by fastd this means: as it is defined over a field with the cardinality $2^{255} - 19$, 255 bit are necessary to store a coordinate. Point compression allows to conveniently pack the 255 bit x coordinate with the least significant bit of the y coordinate into a 256 bit representation.

Even though this optimization is quite obvious, it was protected by US patent 6,141,420 ([VMA00]), which should have complicated the operation of fastd when subject to the US patent law. Fortunately, the patent has expired on 29 July 2014.

3.1.2 The curve used by ec25519

The curve used by ec25519 is based on Curve25519 (see [Ber06]).

Curve25519 uses a Montgomery curve in a reduced representation, which allows very fast scalar multiplication, but makes it impossible to perform simple additions on curve points. Therefore an equivalent twisted Edwards curve is used for fastd.

Curve25519 is defined by the following equation:

$$v^2 = u^3 + 486662u^2 + u$$

over the prime field F_p for the prime $p = 2^{255} - 19$.

[BBJ+08] states that for all Montgomery curves

$$Bv^2 = u^3 + Au^2 + u$$

with $A \in F_p \setminus \{-2, 2\}$ and $B \in F_p \setminus \{0\}$ there is a birationally equivalent twisted Edwards curve

$$ax^2 + y^2 = 1 + dx^2y^2 \text{ with } a = \frac{A+2}{B} \text{ and } d = \frac{A-2}{B},$$

thus leading to the following curve equation:

$$486664x^2 + y^2 = 1 + 486660x^2y^2$$

Generator point

Curve25519 uses a point with

$$u = 9$$

as its generator; the v coordinate is not specified as it is not needed by the algorithm.

The two possible v coordinates are:

$$\begin{aligned} v1 &= 0x20ae19a1b8a086b4e01edd2c7748d14c923d4d7e6d7c61b229e9c5a27eced3d9 \\ v2 &= 0x5f51e65e475f794b1fe122d388b72eb36dc2b28192839e4dd6163a5d81312c14 \end{aligned}$$

3.2.1 Protocol specification

1. The initiator Alice does the following:
 - (a) Choose $x \in [1, q - 1]$ and compute $X = xG$.
 - (b) Send (\hat{A}, \hat{B}, X) to Bob.
2. At the receipt of (\hat{A}, \hat{B}, X) Bob does the following:
 - (a) Verify that $X \in \mathcal{G}^*$.
 - (b) Choose $y \in [1, q - 1]$, compute $Y = yG$.
 - (c) Compute $d = \bar{H}(X, Y, \hat{A}, \hat{B})$ and $e = \bar{H}(Y, X, \hat{A}, \hat{B})$.
 - (d) Compute $s_B = y + eb \pmod q$, $\sigma_B = s_B(X + dA)$.
 - (e) Compute $K_1 = KDF_1(\sigma_B, \hat{A}, \hat{B}, X, Y)$ and $t_B = MAC_{K_1}(\hat{B}, Y)$.
 - (f) Send $(\hat{B}, \hat{A}, Y, t_B)$ to Alice.
3. At the receipt of $(\hat{B}, \hat{A}, Y, t_B)$ Alice does the following:
 1. Verify that $Y \in \mathcal{G}^*$.
 2. Compute $d = \bar{H}(X, Y, \hat{A}, \hat{B})$ and $e = \bar{H}(Y, X, \hat{A}, \hat{B})$.
 3. Compute $s_A = x + da \pmod q$, $\sigma_A = s_A(Y + eB)$.
 4. Compute $K_1 = KDF_1(\sigma_A, \hat{A}, \hat{B}, X, Y)$.
 5. Verify that $t_B = MAC_{K_1}(\hat{B}, Y)$.
 6. Compute $t_A = MAC_{K_1}(\hat{A}, X)$.
 7. Send t_A to Bob.
 8. Compute $K_2 = KDF_2(\sigma_A, \hat{A}, \hat{B}, X, Y)$.
4. At the receipt of t_A , Bob does the following:
 - (a) Verify that $t_A = MAC_{K_1}(\hat{A}, X)$.
 - (b) Compute $K_2 = KDF_2(\sigma_A, \hat{A}, \hat{B}, X, Y)$.
5. The shared session key is K_2 .

The third message allows Bob to ensure that he is actually communicating with Alice before the handshake is completed and thus prevents the attack on PFS described in [Kra05] that affects all 2-message key exchange protocols.

3.2.2 Usage in fastd

fastd performs the FHMVQ-C key exchange on the group specified in [ec25519](#).

FHMVQ-C makes use of several cryptographic hash and key derivation functions that are not given in the specification. fastd uses the following definitions for these functions:

$$\begin{aligned}
 d|e &= \text{SHA256}(Y|X|\hat{B}|\hat{A}) \\
 K_1 &= KDF_1(\sigma, \hat{A}, \hat{B}, X, Y) = \text{HKDF-SHA256}(0 \times 00^{32}, \sigma, \hat{A}|\hat{B}|X|Y, 32) \\
 K_2 &= KDF_2(\sigma, \hat{A}, \hat{B}, X, Y) = \text{HKDF-SHA256}(K_1, \sigma, \hat{A}|\hat{B}|X|Y|method, *)
 \end{aligned}$$

where $V|W$ designates the concatenation of the binary strings V and W and

$$\text{HKDF}(salt, IKM, info, L) = \text{HKDF-Expand}(\text{HKDF-Extract}(salt, IKM), info, L)$$

See [FIPS180] (SHA256), [RFC2104] (HMAC) and [RFC5869] (HKDF) for the specifications of these algorithms.

As one can see, the calculation of d and e deviates from the FHMV-C specification, which uses a hash function \bar{H} with half-width (127 bit in the case of `ec25519-fhmvc`) output, defining d and e as

$$\begin{aligned}d &= \bar{H}(X|Y|\hat{A}|\hat{B}) \\e &= \bar{H}(Y|X|\hat{A}|\hat{B})\end{aligned}$$

fastd uses a single 256 bit hash $\text{SHA256}(Y|X|\hat{B}|\hat{A})$ instead and cuts it into two 128 bit pieces which are used as d and e . This optimization allows reusing the SHA256 implementation that is already used for KDF_1 and KDF_2 and saves one hash calculation.

Furthermore, starting with fastd v11 a *TLV authentication tag* protecting the whole handshake packet is used instead of the values t_A and t_B , which verify the public keys only. To generate this tag, $\text{HMAC-SHA256}(K_1, \cdot)$ is applied to a pseudo TLV record list, which is the same as the TLV record list sent in the actual handshake packet, with the exception of the *TLV authentication tag* value, which is replaced by zeros. This ensures that no part of the handshake after the initial packet has been manipulated, preventing downgrade attacks.

For the exact sequence of handshake packets see [Handshake protocol](#).

3.2.3 Bibliography

3.3 Ciphers

Generally, all ciphers used by fastd are [stream ciphers](#).

This means that the cipher outputs a cipher stream indistinguishable from a random byte stream which can be used to encrypt packets of any length without a need for padding the packet size to a multiple of a block size by just XORing the cipher stream with the packet.

3.3.1 AES128-CTR

The Advanced Encryption Standard is a widely used, highly regarded block cipher specified in [FIPS197].

In counter mode a nonce of up to 12 bytes is concatenated with a 4 byte counter; this value is encrypted with the block cipher to compute 16 bytes of the cipher stream.

AES128 has been chosen in contrast to the stronger variants AES192 and AES256 as hardware acceleration for AES128 is more widely available on embedded hardware. Using this acceleration hardware from userspace through the `alg_if` interface of the Linux kernel is very complex though, so support for it has been removed from fastd again (but may still be used through OpenSSL).

One issue with the AES algorithm is that it is very hard to implement in a way that is safe against cache timing attacks (see [Ber05a] for details). Because of that fastd can make use of two different AES implementations: a very secure, but also very slow implementation from the [NaCl](#) library, and the implementations from OpenSSL (which can either use hardware acceleration like AES-NI, or a fast, but potentially insecure software implementation).

3.3.2 Salsa20(/12)

Salsa20 (see [Ber07]) is a state-of-the-art stream cipher which is very fast and very secure. In contrast to AES, it is easily implementable without any timing side channels.

Salsa20/12 is a variant of Salsa20 which uses only 12 instead of 20 rounds to improve performance. The Salsa20/12 has been chosen for the software profile on the [eSTREAM](#) portfolio in 2011 as it has a very high throughput while providing a very comfortable security margin.

The even more reduced variant Salsa20/8 has also been evaluated for fastd, but the performance gain has been too small to warrant the significantly reduced security.

3.3.3 Bibliography

3.4 Message Authentication Codes

3.4.1 GHASH / Galois/Counter Mode (GCM) / GMAC

The Galois/Counter Mode is a very well-known mode of operation for block ciphers which was specified in [MV04]. GMAC is an authentication-only variant of the algorithm.

While the original specification only considers block ciphers, GCM can also be specified in terms of the Counter mode (CTR) of the block cipher. The counter mode transforms a block cipher into a stream cipher. This allows it to replace the block cipher by any stream cipher while preserving all security guarantees; therefore fastd allows to use GMAC with any supported stream cipher.

One particular issue with GCM/GMAC is that it is hard to implement in software. Usually it is implemented using a lookup table, which might exhibit cache timing side channels. This issue doesn't affect modern x86 CPUs providing the PCLMUL instruction, as PCLMUL allows performing carry-less multiplications without a lookup table.

3.4.2 UHASH / UMAC

The UMAC message authentication code defined in [RFC4418] is a strongly universal hash function, which is formed by defining a universal hash function UHASH and XORing it with a pad generated by a block cipher like AES.

In fastd, the pad can be generated by any supported stream cipher, and the key derivation function specified in the RFC has been replaced by HKDF.

The UHASH function is optimized for efficient implementation in software on 32bit CPUs. Therefore UMAC is much more performant than GMAC, especially on embedded systems, and doesn't exhibit any timing side channels.

3.4.3 Bibliography

3.5 Method providers

See *Encryption & authentication methods* for details about the method configuration and recommendations.

3.5.1 generic-gmac

The *generic-gmac* provider combines the GHASH message authentication code with any stream cipher, which is used both to encrypt the data and the authentication tag.

After the last encrypted data block, a block containing the length of the data (in bits, big endian) is passed to the GHASH function as defined by the GCM specification.

The method names normally have the form “<cipher>+gmac”, and “aes128-gcm” for the AES128 cipher.

3.5.2 composed-gmac

The *composed-gmac* provider combines the GHASH message authentication code with two stream ciphers, where the first one is used to encrypt the data and the second one for the authentication tag. As only the authentication tag must be encrypted, “null” can be used as the first cipher for authenticated-only methods.

After the last encrypted data block, a block with the first 8 bytes containing the length of the data (in bits, big endian) and the other 8 bytes set to zero is passed to the GHASH function. This differs from the size block used by the *generic-gmac* for historical reasons.

The method names normally have the form “<cipher>+<cipher>+gmac”, and “<cipher>+aes128-gmac” for the AES128 cipher.

3.5.3 generic-umac

The *generic-umac* provider combines the UHASH message authentication code with any stream cipher, which is used both to encrypt the data and the authentication tag.

The method names have the form “<cipher>+umac”.

3.5.4 composed-umac

The *composed-umac* provider combines the UHASH message authentication code with two stream ciphers, where the first one is used to encrypt the data and the second one for the authentication tag. As only the authentication tag must be encrypted, “null” can be used as the first cipher for authenticated-only methods.

The method names have the form “<cipher>+<cipher>+umac”.

3.5.5 generic-poly1305

The *generic-umac* provider combines the [Poly1305](#) message authentication code with any stream cipher, which is used both to encrypt the data and the authentication tag. This method was added to replace the deprecated *xsalsa20-poly1305* method, but may be removed as well in the long term as UMAC is generally more performant and makes the same security guarantees.

The method names have the form “<cipher>+poly1305”.

3.5.6 xsalsa20-poly1305

The *xsalsa20-poly1305* provider only provides a single method, “xsalsa20-poly1305”, which uses the “secret box” provided by the [NaCl](#) library. It is deprecated and should be used for connections with very old fastd versions only.

3.5.7 null

The “null” method doesn’t provide any encryption or authentication.

3.5.8 cipher-test

The *cipher-test* method can be used to run a cipher without any authentication. This isn’t secure and should be used for tests and benchmarks only.

The method names have the form “<cipher>+cipher-test”.

Developer documentation

4.1 Protocol specification

4.1.1 Basic protocol design

fastd uses UDP as the transport protocol for its packets. UDP has been chosen instead of raw IP packets (as they are used by IPIP and 6in4 tunnels or IPsec) to simplify the deployment of multiple fastd instances on the same host using different UDP ports and allow passing through common NAT routers without explicit configuration.

The first byte of the UDP payload is used to discern the different packet types used by fastd. For now only two values for the first byte have been defined: `0x01` indicates a handshake packet, and `0x02` a data packet. All other values are reserved for future use and must be ignored by current implementations.

4.1.2 Handshake format

For historical reasons, all multi-byte values mentioned in the handshake specification are transmitted in Little Endian byte order unless specified otherwise.

The initial `0x01` byte together with the next three bytes form the 4-byte handshake header; the rest of the packet after the header consists of a list of TLV records. The second header byte is reserved and must always be `0x00`; the following two header bytes contain the length of the following TLV records in bytes encoded as Big Endian.

The following TLV records start with a 2-byte type field, followed by a 2-byte length field and the arbitrary-length value. There is no special alignment defined for the TLV records.

TLV record types

Record ID	Value description	Format	Values
0x0000	Handshake type	1-byte unsigned integer	{1, 2, 3}
0x0001	Reply code	1-byte unsigned integer	{0 (success), 1 (mandatory record missing), 2 (unacceptable value)}
0x0002	Error detail	1/2-byte unsigned integer	Record type which caused an error
0x0003	Flags (currently unused)	variable-length bit field	So far, no values are defined
0x0004	Mode	1-byte unsigned integer	{0 (TAP mode), 1 (TUN mode)}
0x0005	Protocol name	variable-length string	“ec25519-fhmqvc”
0x0006	Sender key	32-byte public key	Not used if secure handshakes are enabled
0x0007	Recipient key	32-byte public key	
0x0008	Sender handshake key	32-byte public key	
0x0009	Recipient handshake key	32-byte public key	
0x000a	Authentication tag (obsolete)	32-byte opaque value	
0x000b	MTU	2-byte unsigned integer	
0x000c	Method name	variable-length string	
0x000d	Version name	variable-length string	
0x000e	Method list	zero-separated string list	
0x000f	TLV authentication tag	32-byte opaque value	

Handshake protocol

The following specification describes the current handshake as it is performed by fastd versions since v11 when secure handshakes are enabled.

The handshake protocol consists of three packets. See also: *ec25519*, *FHMQV-C*

The following fields are sent in all three packets as different fastd versions expect them in different parts of the handshake:

- Mode (TUN/TAP)
- MTU
- fastd version (e.g. v15)
- Protocol name (ec25519-fhmqvc)

Handshake request

The first packet of a handshake contains the following additional fields:

- Handshake type (0x01)
- FHMV-C values:
 - Sender key \hat{A}
 - Recipient key \hat{B}
 - Sender handshake key X

The recipient key may be omitted if the recipient identity is unknown because the handshake was triggered by an unexpected data packet.

Handshake reply

The second packet of a handshake contains the following additional fields:

- Handshake type (0x02)
- Reply code (0x00)
- Method list (list of all supported methods)
- FHMV-C values:
 - Sender key \hat{B}
 - Recipient key \hat{A}
 - Sender handshake key Y
 - Recipient handshake key X
 - TLV authentication tag MAC_B

Handshake finish

The second packet of a handshake contains the following additional fields:

- Handshake type (0x03)
- Reply code (0x00)
- Method (the chosen encryption/authentication scheme)
- FHMV-C values:
 - Sender key \hat{A}
 - Recipient key \hat{B}
 - Sender handshake key X
 - Recipient handshake key Y
 - TLV authentication tag MAC_A

Handshake error

When an unacceptable handshake is received, fastd will respond with an error packet. The error packet contains the following fields:

- Handshake type (the type of the packet that is answered plus 1)

- Reply code (0x01 when a record is missing from the handshake, 0x02 when a value is unacceptable)
- Error detail (the record type ID which caused the error)

4.1.3 Payload packets

The payload packet structure is defined by the methods; at the moment most methods use the same format, starting with a 24 byte header, followed by the actual payload:

- Byte 1: Packet type (0x02)
- Byte 2: Flags (method-specific; unused, always 0x00)
- Bytes 3-8: Packet sequence number/nonce (big endian; incremented by 2 for each packet; one side of a connection uses the even sequence numbers and the other side the odd ones)
- Bytes 9-24: Authentication tag (method-specific)

The `null` method uses only a 1 byte header: The packet type is directly followed by the payload data.

In the legacy `xsalsa20-poly1305` method, the flag and nonce fields are reversed and the nonce is in little endian for compatibility reasons.

- [BBJ+08] D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, “Twisted Edwards curves”, in Progress in Cryptology—AFRICACRYPT 2008, Springer, 2008, pp. 389–405.
- [Ber06] D. J. Bernstein, “Curve25519: new Diffie-Hellman speed records”, in Public Key Cryptography-PKC 2006, Springer, 2006, pp. 207–228.
- [EFD] D. J. Bernstein and T. Lange, “Explicit-Formulas Database—Genus-1 curves over large-characteristic fields”. [Online] <http://hyperelliptic.org/EFD/g1p/index.html>
- [HWCD08] H. Hisil, K. K.-H. Wong, G. Carter and E. Dawson, “Twisted Edwards curves revisited”, in Advances in Cryptology—ASIACRYPT 2008, Springer, 2008, pp. 326–343.
- [VMA00] S. A. Vanstone, R. C. Mullin and G. B. Agnew, “Elliptic curve encryption systems”, US Patent 6,141,420, 2000.
- [FIPS180] National Institute of Standards and Technology, “Secure hash standards (SHS)”, Federal Information Processing Standard 180-4, 2012. [Online] <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>
- [Kra05] H. Krawczyk, “HMQV: a high-performance secure Diffie-Hellman protocol”, Cryptology ePrint Archive, Report 2005/176, <http://eprint.iacr.org/>, 2005.
- [LMQ+98] L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, “An efficient protocol for authenticated key agreement”, Designs, Codes and Cryptography, vol. 28, pp. 361–377, 1998.
- [RFC2104] H. Krawczyk, M. Bellare and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104 (Informational), Updated by RFC 6151, Internet Engineering Task Force, 1997. [Online] <http://www.ietf.org/rfc/rfc2104.txt>
- [RFC5869] H. Krawczyk and P. Eronen, “HMAC-based Extract-and-Expand Key Derivation Function (HKDF)”, RFC5869 (Informational), Internet Engineering Task Force, 2010. [Online] <http://www.ietf.org/rfc/rfc5869.txt>
- [SEB09] A. P. Sarr, P. Elbaz-Vincent and J. Bajard, “A secure and efficient authenticated Diffie-Hellman protocol”, Cryptology ePrint Archive, Report 2009/408, <http://eprint.iacr.org/>, 2009.
- [Ber05a] D. J. Bernstein, “Cache-timing attacks on AES”, 2005. [Online] <http://cr.yp.to/antiforgery/cachetiming-20050414.pdf>
- [Ber07] D. J. Bernstein, “The Salsa20 family of stream ciphers”, 2007. [Online] <http://cr.yp.to/snuffle/salsafamily-20071225.pdf>
- [FIPS197] National Institute of Standards and Technology, “ADVANCED ENCRYPTION STANDARD (AES)”, Federal Information Processing Standard 197, 2001. [Online] <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

- [MV04] D. McGrew and J. Viega, “The Galois/counter mode of operation (GCM)”, Submission to NIST Modes of Operation Process, 2004.
- [RFC4418] T. Krovetz, “UMAC: Message Authentication Code using Universal Hashing”, RFC4418 (Informational), Internet Engineering Task Force, 2006. [Online] <http://www.ietf.org/rfc/rfc4418.txt>