VERSION: 0

<table>
<tr><th colspan="34">DEFAULT Packet</th></tr>
<tr><td>*Offsets*</td><td>Octet</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Octet</td><td>Bit</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>0</td><td>0</td><td colspan="4">Version</td><td colspan="4">Type</td><td colspan="8">Flags</td><td colspan="16">Sequence ID</td></tr>
<tr><td>4</td><td>32</td><td colspan="8">Fragment ID*</td><td colspan="8">Fragment Number*</td><td colspan="16">Init Vector*</td></tr>
<tr><td>8</td><td>64</td><td colspan="16">Checksum Hash*</td><td colspan="16">*Data**</td></tr>
</table>

<table>
<tr><th colspan="34">ACK Packet</th></tr>
<tr><td>*Offsets*</td><td>Octet</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Octet</td><td>Bit</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>8</td><td>64</td><td colspan="16">*Default Packet Headers*</td><td colspan="16">ACK ID</td></tr>
<tr><td>12</td><td>96</td><td colspan="16">ACK Bits</td><td colspan="16">*Data**</td></tr>
</table>

<table>
<tr><th colspan="34">AUTH Packet</th></tr>
<tr><td>*Offsets*</td><td>Octet</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Octet</td><td>Bit</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>8</td><td>64</td><td colspan="16">*Default Packet Headers*</td><td colspan="8">Reserved</td><td colspan="8">EC Public Key Size (**E**)</td></tr>
<tr><td>12</td><td>96</td><td colspan="32">EC Public Key</td></tr>
<tr><td>...</td><td>...</td><td colspan="32">...</td></tr>
<tr><td>10+E</td><td>80+E</td><td colspan="16">EC Public Key</td><td colspan="16">Certificate Size (**C**)*</td></tr>
<tr><td>14+E</td><td>168+E</td><td colspan="32">Certificate*</td></tr>
<tr><td>...</td><td>...</td><td colspan="32">...</td></tr>
<tr><td>12+C+E</td><td>96+C+E</td><td colspan="16">Certificate*</td><td colspan="16"></td></tr>
</table>

**Not required*

*Note: **C** and **B** are in bytes*

HEARTBEAT Packet																																	
Offsets	**Octet**	**0**								**1**								**2**								**3**							
Octet	Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
8	**64**	*Default Packet Headers*																Heartbeat								*Data**							

ERROR Packet																																	
Offsets	**Octet**	**0**								**1**								**2**								**3**							
Octet	Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
8	**64**	*Default Packet Headers*																Error Major				Error Minor				*Data**							

**Not required*

Types

Type	Enum
DEFAULT	0
ACK	1
AUTH	2
HEARTBEAT	3
ERROR	4
RESERVED	4..15

Flags

Octet	1							
Bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Flag	RELIABLE	CHECKSUM	COMPRESSED	ENCRYPTED	FRAG	RESERVED		

Note: packet should be encoded in flag order and decoded in reverse

Error Codes

Major	Minor	Name	Description
1	**0**	**CONNECTION**	**Connection Handshake Could Not Finish**
	1	NO SPACE	Server has no more space
	2	CERTIFICATE INVALID	Certificate is invalid / cannot be validated
	3	FINISH INVALID	Finished is invalid
2	**0**	**DISCONECT**	**A Party is Disconnecting**
	1	SERVER DISCONECT	The server is closing, all clients must exit gracefully
	2	CLIENT DISCONECT	The client is closing, the server must handle gracefully
3	**0**	**PACKET**	**The Packet Cannot be Read**
	1	VERSION	The packet version does not match the expected
	2	PACKET TYPE	Unknown / invalid packet type
	3	FLAGS	Unknown / invalid flags
	4	SEQUNCE ID	Sequence id does not match expected
	5	FRAGMENT ID	Unknown / invalid fragment id
	6	FRAGMENT NUMBER	Unknown / invalid fragment number
	7	INIT VECTOR	Unknown / invalid init vector i.e. decrypt fail
	8	COMPRESSION	Decompression fail
	9	CHECKSUM	Unknown / invalid checksum i.e. checksum fail
4..15		**RESERVED**	

Default Packet Spec

Field	Size	Required	Required Flags	Notes
Version	4	1		Version number. 0 (zero) for all development.
Type	4	1		See Types.
Flags	8	1		See Flags.
Sequence ID	16	1		Packet identification number set by the sender.
Fragment ID*	8	0	FRAG	Position in reassembled packed.
Fragment Number*	8	0	FRAG	Total number of fragmented packed.
Init Vector*	16	0	ENCRYPT	Init vector for use when decrypting.
Checksum Hash*	16	0	CHECKSUM	CRC-32 checksum.
*Data**		0		Data can be length 0..988 bytes .

ACK Packet Spec

Field	Size	Required	Required Flags	Notes
Default Packet Headers	36-80	1		See Default Packet Spec.
ACK ID	16	1		The Sequence ID (see Default Packet Spec) of a packet with RELIABLE (see flags).
ACK Bits	16	1		A record of the local ACK Bits such that [ACK ID-1, ACK ID-2 ... ACK ID-17]
*Data**		0		Data can be length 0..988 bytes. Used to send finished in handshake

AUTH Packet Spec

Field	Size	Required	Required Flags	Notes
Default Packet Headers	36-80	1		See Default Packet Spec.
Reserved	8	1		For padding.
EC Public Key Size (**E**)	8	1		Size of EC Public Key in *bytes* .
EC Public Key	**E**	1		Senders Public Elliptic Curve Key (for generating session key).
Certificate Size (**C**)*	16	0		Size of Certificate in *bytes* .
Certificate*	**C**	0		Senders Certificate (for identity validation).

*Not required

*Note: **C** and **B** are in bytes*

HEARTBEAT Packet Spec

Field	Size	Required	Required Flags	Notes
Default Packet Headers	36-80	1		See Default Packet Spec.
Heartbeat	8	1		Boolean: False indicates PING, True indicates PONG.
*Data**		0		Data can be length 0..988 bytes.

ERROR Packet Spec

Field	Size	Required	Required Flags	Notes
Default Packet Headers	36-80	1		See Default Packet Spec.
Error Major	4	1		See Error Codes.
Error Minor	4	1		See Error Codes. Must be present but can be all 0.
*Data**		0		Data can be length 0..988 bytes. Additional error message (for logging / client)

**Not required*