**Legend:**

|  |
| --- |
| 30 Byte |
| Username |

**Authentication phase:**

|  |  |
| --- | --- |
| 16 Byte |  |
| Ns | Certs |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 12 Byte | 16 Byte |  |  | | |
| Enc\_key | IV | Nc | Yc | Nc | Ns | Yc |

Enc\_key, IV, {Nc, Yc, <Nc, Ns, Yc>Prvk\_c }Pubk\_s

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 12 Byte |  |  | | |
| Enc\_key | IV | Ys | Nc | Ns | Ys |

Enc\_key, IV, {Ys, <Nc, Ns, Ys>Prvk\_s }Pubk\_c

**Legend:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | Variable |
| IV | AAD | Tag | Type | Payload |

**Upload:**

**C🡪S**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | 30 Byte | 32 Byte |
| IV | AAD | Tag | upl | filename | size |

**S 🡪 C**

**ack**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | ack |

**nack**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | not |

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | (max) 1 MByte |
| IV | AAD | Tag | Payload |

**Download:**

**C 🡪 S**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | 30 Byte |
| IV | AAD | Tag | dow | filename |

**S 🡪 C**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | 32 Byte |
| IV | AAD | Tag | siz | size |

\*\* se size==0 🡪 Nack

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | (max) 1 MByte |
| IV | AAD | Tag | Payload |

**Delete:**

**C 🡪 S**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | 30 Byte |
| IV | AAD | Tag | del | filename |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | ask |

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | ack |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | ack |

**List:**

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | lre |

**S 🡪 C**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 8 Byte |
| IV | AAD | Tag | 0x06 | size |

**S 🡪 C**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | Variable |
| IV | AAD | Tag | lfi | Payload |

**Rename:**

**C 🡪 S**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | 30 Byte | 30 Byte |
| IV | AAD | Tag | ren | Old filename | New filename |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | ack |

**Logout:**

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | log |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte |
| IV | AAD | Tag | ack |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 4 Byte | Variable |
| IV | AAD | Tag | Type | Payload |

Type of messages

* Update\_request upl
* Acknowledgment ack
* Not\_acknowledgment not
* Download\_request dow
* Size siz
* Delete\_request del
* Ask\_confirmation ask
* List\_request lre
* List\_file lfi
* Rename\_request ren
* Logout\_request log