**Legend:**

|  |
| --- |
| Username |

**Authentication phase:**

|  |  |
| --- | --- |
| Ns | Certs |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Enc\_key | IV | Nc | Yc | Nc | Ns | Yc |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | 1 Byte | Variable |
| IV | AAD | Tag | Type | Payload |

**Upload:**

**C🡪S**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 50 Byte | 8 Byte |
| IV | AAD | Tag | 0x01 | filename | size |

**S 🡪 C**

**ack**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x02 |

**nack**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x03 |

**C 🡪 S**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 500 MByte |
| IV | AAD | Tag | 0x04 | Payload |

**Download:**

**C 🡪 S**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 50 Byte |
| IV | AAD | Tag | 0x05 | filename |

**S 🡪 C**

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

\*\* se size==0 🡪 Nack

**S 🡪 C**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 500 MByte |
| IV | AAD | Tag | 0x04 | Payload |

**Delete:**

**C 🡪 S**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 50 Byte |
| IV | AAD | Tag | 0x07 | filename |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x08 |

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x02 |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x02 |

**List:**

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x09 |

**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 | 1 Byte | Variable |
| IV | AAD | Tag | 0x10 | Payload |

**Rename:**

**C 🡪 S**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | 50 Byte | 50 Byte |
| IV | AAD | Tag | 0x11 | Old filename | New filename |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x02 |

**Logout:**

**C 🡪 S**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x12 |

**S 🡪 C**

|  |  |  |  |
| --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte |
| IV | AAD | Tag | 0x02 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12 Byte | 12 Byte | 16 Byte | 1 Byte | Variable |
| IV | AAD | Tag | Type | Payload |

Type of messages

* Update\_request 0x01
* Acknowledgment 0x02
* Not\_acknowledgment 0x03
* File\_content 0x04
* Download\_request 0x05
* Size 0x06
* Delete\_request 0x07
* Ask\_confirmation 0x08
* List\_request 0x09
* List\_file 0x10
* Rename\_request 0x11
* Logout\_request 0x12