Protocol Spezifications

Verbindungsaufbau

Was	Laenge (bytes)	Beispiel
magic	4	k3gV
Version	1	(byte)12
NONCE	8	(long) 4848787
my Port	unsigned short (2 bytes)	59558

Befehle ohne vorgeschriebene Reihenfolge

Was	Befehl (1 byte)	laenge (content)	Beispiel/Beschreibung
	0		fuer was cooles
get PeerList	1	0	anfrage der PeerList
peerlist	2	-	hiermit wird die PeerList ruber geschickt 1. byte: anzahl der IPv4 Adressen 2. byte: anzahl der IPv6 Adressen IPv4: 4 bytes + 2 bytes (unsigned short) fuer Port IPv6: 16 bytes + 2 bytes (unsigned short) fuer Port (x:x:x:x:x:x:x:x, where the 'x's are the hexadecimal values of the eight 16-bit pieces of the address)

Sync	3	-	1. Timestamp to max from both sides since when to sync. If equals to -1, means full sync. (1 long) 2. Count on how much public addresses will follow. If equals to 0, means all addresses. (1 byte) 3. public Address to sync (33 byte each)
Address to ID	4	36 bytes	1. public address (33 byte) 2. id (int)
Have Message	5	21 byte	1. id (int) 2. public message type (byte) 3. timestamp (long) 4. nonce (int) 5. messageId (int)
Get Message	6	4 byte	message id (int)
Message content (message type = 20 oder > 50)	7	-	1. id (int) 2. signature (72 byte) 3. groesse des contents, also anz. der bytes (unsigned int, 4 byte) 4. content
Get control data for TrustedData.	8		
Send control data	9		
dns peer / IPv6 hack	10	-	1. byte laenge des Strings -> max 256 2. String host dns or ipv6 3. 2 bytes (unsigned short) fuer Port

request Auth Key	51	16	Zum einigen auf ein neuen AuthKey. Der die Verbindung aufbaut bestimmt die ersten 16 bytes, der andere die letzten. 1. 16 byte fuer eine haelfte des Schluessels
auth now	52	32	Hiermit wird versucht die andere Seite zu identifizieren. Sollten 32 byte an zufaelligen Daten sein. Der der den Befehl empfaengt muss diese mit dem gemeinsamen AuthKey verschluesseln (AES 256). 1. 32 byte zufaellige Daten.
auth answer	53	32	Verschluesselte 32 bytes. Falls dies nun fehlschlaegt, wird der Befehl request AuthKey gesendet und ein neuer Schluessel erstellt. Achtung NONCEN sind nicht eindeutig zum den trusted Daten aufloesbar. Deswegen muss eventuell ein anderer AuthKey verwendet werden und nicht direkt ein neuer beantragt werden. Dies wird aber ersichtlich durch das Authen von der anderen Partei.
aktiviere RC4	55		ab nun wird dieser Strom verschluesselt mit dem erstellten RC4 schluessel...

addFilterMessage	60		Public Key von welchem Nachrichten erwünscht sind. Alle anderen werden nicht angenommen. 1. Key ID siehe (byte) 4, ein Integer 2. ~~Eventuelle Erweiterung mit Priorität?~~
set Client Type	61		1. type (int), Types are: 0 - supernode (root), 1 - normal client (normal PC), 2 - light client (smartphone)
ping	100	0	request pong answer
pong	101	0	answer from ping
Sticks	150	-	Fuer die Beschreibung der Sticks siehe Seite Sticks.
disconnect	254	0	disconnect from peer
protocol error	255	0	disconnect + remove peer, an fatal error occured.