

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00	magic <b>0xDEC0DE</b>				counter <b>1</b>				type <b>3</b>	payload size <b>8 + keylen</b>				random nonce... <b>N<sub>A</sub><sup>5</sup></b>			
10	..rand nonce	previous hash... <b>...00000...</b>															
20	...previous hash... <b>...00000...</b>																
30	..prev hash	DH nonce <b>N<sub>DH</sub><sup>AB</sup></b>				keylen <b>N</b>				DH key...							
40	...DH key...																
⋮																	
	signature size				message signature...												
	...message signature...																