Simple but longterm card-terminal authorization protocol based on one time passwords - sketch of protocol

Card	Transmission	Terminal
		Sends Hello Messsage and asks card for authentication.
	1. $\leftarrow HelloMessage$	
Generates the challenge nonce (NC).		
	2.$NC \rightarrow$	
		Prepare the challenge nonce (NR). Respond on NC nonce with AR value. Cipher both nonce and value with KeyStream.
	3. $\leftarrow KeyStream1 \oplus NR + KeyStream2 \oplus AR$	
Deciphers the response, verifies the challenge AR and responds with AC value. Also sends current State of card. Everything is ciphered with usage of the same KeyStream.		
	4.$AC \oplus KeyStream3$, $State \oplus KeyStream4 \rightarrow$	
		Verify the AC challange. Verify the state. Send new state.
	5. $\leftarrow NewState \oplus KeyStream5$	
Save the new state.		

To detect the attemp of relay attack the terminal is gathering the informations about the delays between each card response (in miliseconds). If the sum of delays is higher than given safe value, the card is revoked on the end of authentication procedure.