C		S
	$\xrightarrow[\text{OPTIONAL}]{\text{Hello}}$	
		S periodically decides k, generates N_S, and timestamps and signs the following message.
	$\xleftarrow[\text{BROADCAST}]{S_S(T_S, k, N_S)}$	
C verifies the timestamp T_S and signature S_S. If N_S is new, C sets $i_C = 0$. Otherwise, C increments i_C. C solves X by brute force from $h(C, N_S, i_C, X) = 0_1 0_2 \ldots 0_k Y$. C generates N_C and signs the following message.		
	$\xrightarrow{S_C(S, C, N_S, i_C, X, N_C)}$	
		S verifies that N_S is recent, C, N_S, i_C not used before, and $h(C, N_S, i_C, X) = 0_1 0_2 \ldots 0_k\ Y$. **S may now commit resources.** S verifies the signature S_C and stores C, N_S, i_C while N_S recent. **S has now authenticated C.** S signs the following message.
	$\xleftarrow{S_S(S, C, N_C)}$	
C verifies the signature S_S. **C has now authenticated S.**		