Client C	*Gateway G*	*Authentication Server S*
$pw \in \mathcal{D}$		$pw \in \mathcal{D}$
$RSA\ keys: n, e, d$	$RSA\ keys: n', e', d'$	
unauthenticated channel	authenticated private channel	
accept $\leftarrow$ false	accept $\leftarrow$ false	
$r_1 \in_R \{0,1\}^k$		
$\xrightarrow{C, n, e, r_1}$	$\xrightarrow{C, n, e, n', e', r_1}$	
		e 80-bit prime? and n odd?
		if not, reject. otherwise,
		$x_1, x_2 \in_R Z_n^*, r_2 \in_R \{0,1\}^k$
		$y_1 = x_1^e \bmod n$, $y_2 = x_2^e \bmod n$
		$w = H(pw, x_2, ID_1)$
		$ID_1 = (C, G, n, e, n', e', r_1, r_2, y_2)$
		if $gcd(w, n) \neq 1$, reject
		$z = y_1 \cdot w \bmod n$
$\xleftarrow{G, n', e', r_2, z, y_2}$	$\xleftarrow{r_2, z, y_2}$	
n' odd?		
$b_1 \in_R Z_{n'}^*$, $x_2 = y_2^d \bmod n$		
$w = H(pw, x_2, ID_1)$		
if $gcd(w, n) \neq 1$, reject		
$c_1 = b_1^{e'} \bmod n'$		
$x_1 = (w^{-1} \cdot z)^d \bmod n$		
$\mu = H_1(x_1, ID_1, z, c_1)$		
$\xrightarrow{C, c_1, \mu}$	$b_2 \in_R Z_n^*$	
	$c_2 = b_2^e \bmod n$	
	$\xrightarrow{C, c_1, c_2, \mu}$	μ valid?
		$\eta = H_2(x_1, ID_1, ID_2)$
	$\xleftarrow{\eta}$	$ID_2 = (z, c_1, c_2)$
	$b_1 = c_1^{d'} \bmod n'$	
$\xleftarrow{G, \eta, c_2}$		
η valid?	$sk \leftarrow H_3(b_1, b_2, ID)$	
$b_2 = c_2^d \bmod n$	$ID = (ID_1, ID_2)$	
$sk \leftarrow H_3(b_1, b_2, ID)$		
accept $\leftarrow$ true	accept $\leftarrow$ true	