Generación de Certificados

Usuario/Servidor	Tx/Rx	Autoridad certificadora
Generar números aleatorios d		Generar números aleatorios c
Generar llaves Q = d X P		Obtener llaves (R, k)
Enviar llave pública Q	>>>>>	Recibir llave pública Q
Generar hash e = H(Q)		Generar hash e = H(Q)
		Generar firma (r, s) = (e + kc)
Recibir llave pública (R)	<<<<<	Enviar llave pública (R)
Recibir firma (r, s)	<<<<<	Enviar firma (r, s)
Guardar (d, Q, R, e, (r, s))		

Autenticación Mutua y Acuerdo de Llaves

Usuario	Tx/Rx	Servidor
Obtener (d_u, Q_u, R, e_u, (r_u, s_u))		Obtener (d_s, Q_s, R, e_s, (r_s, s_s))
Cifrar datos $C_u = E(Q_u, e_u, (r_u, s_u))$		Cifrar datos $C_s = E(Q_s, e_s, (r_s, s_s))$
Recibir datos cifrados C_s	<<<<<	Enviar datos cifrados C_s
Enviar datos cifrados C_u	>>>>>	Recibir datos cifrados C_u
Descifrar datos $(Q_s, e_s, (r_s, s_s)) = D(R, C_s)$		Descifrar datos $(Q_u, e_u, (r_u, s_u)) = D(R, C_u)$
Verificar firma (e_s, (r_s, s_s))		Verificar firma (e_u, (r_u, s_u))
Si firma == OK => continua, si no => termina		Si firma == OK => continua, si no => termina
Generar llave mutua ($Q_k = d_u$ X Q_s)		Generar llave mutua ($Q_k = d_s$ X Q_u)