```
role server(S,Ui:agent,SKas:symmetric_key,H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by S
def=
local State:nat,
ID,Pw,G,VPw,B,N,P,K,Cs,T,Cu,Vs,W:text,
Ru,A,Au,V,Fu,Zu,Su,SK,Auths:message,
Inc:hash_func
const alice_server,server_alice,subs1,subs2,
subs3,subs4,subs5,subs6,subs7:protocol_id
init State:=0
transition
1.State=0/\Rcv(ID')=|>
State':=1
/\A':=new()
/\N':=H(K.ID.B)
/\VPw':=H(Pw.A'.ID)
/\Au':=H(xor(H(ID),VPw))
/\Ru':=xor(N,VPw')
/\secret({B},subs4,{S})
/\secret({K},subs5,{S})
/\Snd({A'.Au'.Ru'}_SKas)
2.State=1/\Rcv(V'.Fu'.Zu')=|>
State':=2
/\Cs':=new()
/\T':=new()
/\Vs':=Mul(Cs'.V')
/\Su':=Mul(Cs'.G)
/\SK':=H(N.W.Fu'.Vs'.ID.T')
/\Auths':=H(T'.SK'.N)
/\witness(S,Ui,server_alice_cs,Cs')
/\secret({Cs'},subs6,{Ui,S})
/\secret({SK'},subs7,{Ui,S})
/\Snd(Su'.Auths'.T')
end role
```