A trace has been found.
Abbreviations
~X_1 = aenc(((a_1,revoke_request),sign((a_1,revoke_request),
~M_2),~M_3),~M)
= aenc(((a_1,revoke_request),sign(
(a_1,revoke_request),attsk_2),cert(attvid_2,pk(
attsk_2),cask_3)),pk(cask_3))
Honest Process
Attacker
{1}new gmsk_4
{2}new cask_3
~M = pk(cask_3)
!
!
!
{5}new vid_7
{6}new vsk_3
{91}new attvid_2
{92}new attsk_2
{95}event AttackerGetsEnrollmentCertificate(attvid_2,
pk(attsk_2))
Beginning of process CARevoke
(~M_1,~M_2,~M_3) = (attvid_2,attsk_2,cert(attvid_2,
pk(attsk_2),cask_3))
Beginning of process VehicleRegistration
{14}event ValidGroupKeyRequestSent(vid_7)
~M_4 = aenc((groupkey_request,sign(groupkey_request,
vsk_3),cert(vid_7,pk(vsk_3),cask_3)),pk(cask_3))
~X_1
{153}get revokedcerts(=attvid_2): else branch taken
{126}event ValidRevocationReportReceived(a_1,cert(
attvid_2,pk(attsk_2),cask_3))