

A trace has been found.

Honest ProcessAttacker

{1}new skCA\_1

~M = pk(skCA\_1)

{4}new skRogueCA\_1

(~M\_1,~M\_2) = (pk(skRogueCA\_1),skRogueCA\_1)

{7}new skServer\_3  
{8}new subjectServer\_1

~M\_3 = cert(subjectServer\_1,pk(skServer\_3),skCA\_1)

{12}new skServer2\_1  
{13}new subjectServer2\_1

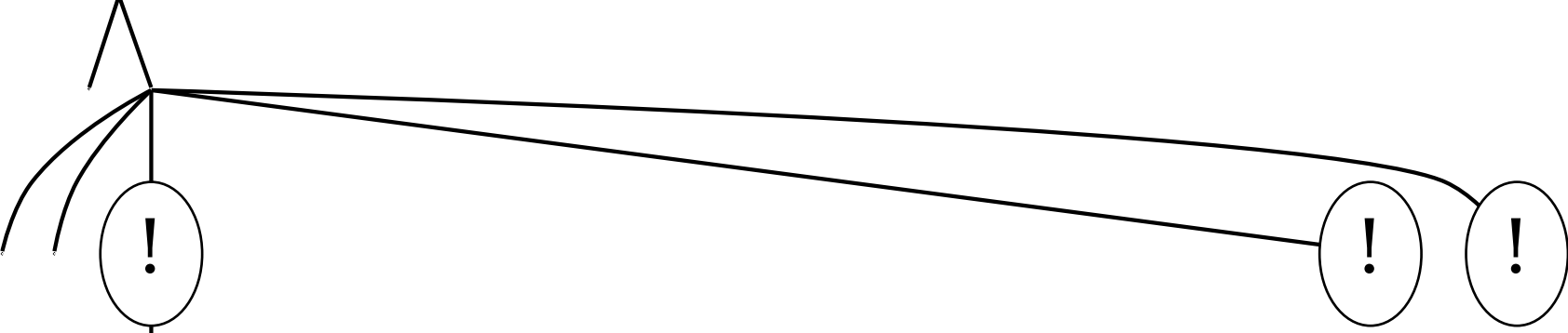
~M\_4 = cert(subjectServer2\_1,pk(skServer2\_1),skCA\_1)

{17}new skServerAttacker\_1

(~M\_5,~M\_6) = (cert(subjectServer\_1,pk(skServerAttacker\_1),  
skRogueCA\_1),skServerAttacker\_1)

{21}new path\_1

~M\_7 = certDevice(subjectServer\_1,constructURL(  
subjectServer\_1,path\_1),skRogueCA\_1)



Beginning of process Thing  
{109}event thingSentURL(constructURL(subjectServer\_1,  
path\_1))

~M\_8 = certDevice(subjectServer\_1,constructURL(  
subjectServer\_1,path\_1),skCA\_1)

{111}event endThing