

Abbreviations
$\sim M_8 = \text{certDevice}(\text{subjectServer}_1, \text{constructURL}(\text{subjectServer}_1, \text{path}_1), \text{pk}(\text{skThingAttacker}_1), \text{skRogueCA}_1)$
$\sim M_9 = \text{skThingAttacker}_1$
$\sim X_1 = \text{PRF}(\text{PRF}(a_3, a_1, \sim M_{11}), \text{client_finished_label}, \text{hash}((a_1, \sim M_{11}, \sim M_5, \text{penc}(a_3, \text{getPkServer}(\sim M_5))))))$ $=$ $\text{PRF}(\text{PRF}(a_3, a_1, \text{serverRandom}_4), \text{client_finished_label}, \text{hash}((a_1, \text{serverRandom}_4, \text{cert}(\text{subjectServer2}_1, \text{pk}(\text{skServer2}_1), \text{skCA}_1), \text{penc}(a_3, \text{pk}(\text{skServer2}_1))))))$
$\sim M_{13} = \text{PRF}(\text{PRF}(a_3, a_1, \text{serverRandom}_4), \text{server_finished_label}, \text{hash}(((a_1, \text{serverRandom}_4, \text{cert}(\text{subjectServer2}_1, \text{pk}(\text{skServer2}_1), \text{skCA}_1), \text{penc}(a_3, \text{pk}(\text{skServer2}_1))))), \text{PRF}(\text{PRF}(a_3, a_1, \text{serverRandom}_4), \text{client_finished_label}, \text{hash}((a_1, \text{serverRandom}_4, \text{cert}(\text{subjectServer2}_1, \text{pk}(\text{skServer2}_1), \text{skCA}_1), \text{penc}(a_3, \text{pk}(\text{skServer2}_1)))))))$
$\sim X_2 = (\text{getURL}(\sim M_{10}), \text{HMAC}(\text{getURL}(\sim M_{10}), \text{PRF}(\text{PRF}(a_3, a_1, \sim M_{11}), \sim M_{11}, a_1)))$ $= (\text{constructURL}(\text{subjectServer2}_1, \text{path}_1), \text{HMAC}(\text{constructURL}(\text{subjectServer2}_1, \text{path}_1), \text{PRF}(\text{PRF}(a_3, a_1, \text{serverRandom}_4), \text{serverRandom}_4, a_1)))$

A trace has been found.

