

Abbreviations
$\sim M_5 = \text{aenc}(\text{make\_presentation}(didTPP,a_4),\text{make\_credential}(didU,didTPP,\text{READ\_PERMISSION}),\text{sign}((didU,didTPP,\text{READ\_PERMISSION}),\text{skU}))$ , $\sim M_6 = \text{aenc}(\text{make\_presentation}(didTPP,a_4),\text{make\_credential}(didU,didTPP,\text{READ\_PERMISSION}),\text{sign}((didU,didTPP,\text{READ\_PERMISSION}),\text{skU})))$ , $\sim X_1 = \text{aenc}(\text{make\_presentation}(didTPP,3\text{-proj-3-tuple}(\text{adec}(\sim M_8,a_7)),3\text{-proj-3-tuple}(\text{resolve\_presentation}(\text{adec}(\sim M_5,a_1),\sim M_4)),\text{sign}((didTPP,3\text{-proj-3-tuple}(\text{adec}(\sim M_8,a_7),3\text{-proj-3-tuple}(\text{resolve\_presentation}(\text{adec}(\sim M_5,a_1),\sim M_4))),a_7)),\sim M_6))$ $= \text{aenc}(\text{make\_presentation}(didTPP,\text{nonceB}_4),\text{make\_credential}(didU,didTPP,\text{READ\_PERMISSION}),\text{sign}((didU,didTPP,\text{READ\_PERMISSION}),\text{skU})),\text{sign}((didTPP,\text{nonceB}_4),\text{make\_credential}(didU,didTPP,\text{READ\_PERMISSION}),\text{sign}((didU,didTPP,\text{READ\_PERMISSION}),\text{skU}))),a_7),\text{pk}(\text{skB}))$

A trace has been found.

