

Abbreviations
$\sim M_4 = \text{make_presentation}(\text{didB}, \text{didU}, a_3, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB})), \text{sign}((\text{didB}, \text{didU}, a_3, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB}))), \text{skB}))$
$\sim X_1 = \text{aenc}(\text{make_presentation}(a_6, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M_5, a_4), 4\text{-proj-4-tuple}(\text{resolve_presentation}(\sim M_4, \sim M_1)), \text{sign}((a_6, \text{didU}, 3\text{-proj-3-tuple}(\text{adec}(\sim M_5, a_4), 4\text{-proj-4-tuple}(\text{resolve_presentation}(\sim M_4, \sim M_1))), a_4)), \sim M_2) = \text{aenc}(\text{make_presentation}(a_6, \text{didU}, \text{nonceB}_4, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB})), \text{sign}((a_6, \text{didU}, \text{nonceB}_4, \text{make_credential}(\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}, \text{sign}((\text{didB}, \text{didU}, \text{dataU}, \text{null_cred}), \text{skB}))), a_4)), \text{pk}(\text{skB}))$
$\sim M_1 = \text{pk}(\text{skU})$
$\sim M_2 = \text{pk}(\text{skB})$
$\sim M_3 = \text{aenc}((\text{didU}, \text{didU}, \text{pk}(\text{skU})), \text{pk}(\text{skB}))$
$\text{aenc}((\text{didU}, \text{didU}, a_3), \sim M_1) = \text{aenc}((\text{didU}, \text{didU}, a_3), \text{pk}(\text{skU}))$
$\sim M_4 = \text{aenc}((\text{didU}, \text{didU}, \text{pk}(a_4)), \sim M_2) = \text{aenc}((\text{didU}, \text{didU}, \text{pk}(a_4)), \text{pk}(\text{skB}))$
$\sim M_5 = \text{aenc}((\text{didU}, \text{didU}, \text{nonceB}_4), \text{pk}(a_4))$
$\sim X_1$
$\sim M_6 = a_6$
$\sim M_7 = \text{aenc}(\text{tokenU}, \text{pk}(a_4))$

A trace has been found.

