

Abbreviations
$\sim M_5 = \text{aenc}(\text{make_presentation}(\text{didTPP}, a_4, \text{make_credential}(\text{didU}, \text{didTPP}, \text{READ_PERMISSION}, \text{sign}((\text{didU}, \text{didTPP}, \text{READ_PERMISSION}), \text{skU})), \text{sign}((\text{didTPP}, a_4, \text{make_credential}(\text{didU}, \text{didTPP}, \text{READ_PERMISSION}, \text{sign}((\text{didU}, \text{didTPP}, \text{READ_PERMISSION}, \text{skU}))), \text{skTP}))), \text{pk}(a_1))$
$\sim X_1 = \text{aenc}(\text{make_presentation}(\text{didTPP}, 3\text{-proj-3-tuple}(\text{adec}(\sim M_8, a_7)), 3\text{-proj-3-tuple}(\text{resolve_presentation}(\text{adec}(\sim M_5, a_1), \sim M_4)), \text{sign}((\text{didTPP}, 3\text{-proj-3-tuple}(\text{adec}(\sim M_8, a_7)), 3\text{-proj-3-tuple}(\text{resolve_presentation}(\text{adec}(\sim M_5, a_1), \sim M_4))), a_7)), \sim M_6) \\ = \text{aenc}(\text{make_presentation}(\text{didTPP}, \text{nonceB_4}, \text{make_credential}(\text{didU}, \text{didTPP}, \text{READ_PERMISSION}, \text{sign}((\text{didU}, \text{didTPP}, \text{READ_PERMISSION}), \text{skU})), \text{sign}((\text{didTPP}, \text{nonceB_4}, \text{make_credential}(\text{didU}, \text{didTPP}, \text{READ_PERMISSION}, \text{sign}((\text{didU}, \text{didTPP}, \text{READ_PERMISSION}, \text{skU}))), a_7))), \text{pk}(\text{skB}))$

