| Abbreviations |
| --- |
| ~X_1 = Request(Header(~M_12051,~M_12052,~M_12053,~M_12054, ~M_12055),~M_12044,CoAP_Option_OSCORE_Option_context( ~M_12048,~M_12049,~M_12050),payload_from_ciphertext( ~M_12047)) = Request(Header(CoAP_versionOne,CoAP_nonConfirm, CoAP_tokenLength(token_10591),CoAP_GETCode,messageID_10592), token_10591,CoAP_Option_OSCORE_Option_context( partial_iv_10589,IDir_10590,idcontext_10588),payload_from_ciphertext( enc_COSE_ciphertext(derive_key_context(MasterSecret_10587, IDir_10590,default_aead_algorithm,idcontext_10588), aead_nonce(IDir_10590,derive_common_iv_context( MasterSecret_10587,idcontext_10588,default_aead_algorithm), partial_iv_10589),(CoAP_POSTCode,payload_10593), AAD(encrypt0_context,encrypt0(oscore_version_one, default_aead_algorithm,IDir_10590,partial_iv_10589))))) |
| ~X_2 = Request(Header(a_10579,a_10580,a_10581,a_10582, a_10583),a_10584,CoAP_Option_OSCORE_Option_context( ~M_12048,~M_11516,~M_11518),payload_from_ciphertext( ~M_12047)) = Request(Header(a_10579,a_10580,a_10581, a_10582,a_10583),a_10584,CoAP_Option_OSCORE_Option_context( partial_iv_10589,IDir_10590,idcontext_10588),payload_from_ciphertext( enc_COSE_ciphertext(derive_key_context(MasterSecret_10587, IDir_10590,default_aead_algorithm,idcontext_10588), aead_nonce(IDir_10590,derive_common_iv_context( MasterSecret_10587,idcontext_10588,default_aead_algorithm), partial_iv_10589),(CoAP_POSTCode,payload_10593), AAD(encrypt0_context,encrypt0(oscore_version_one, default_aead_algorithm,IDir_10590,partial_iv_10589))))) |
| ~X_3 = Request(Header(a_10579,a_10580,a_10581,a_10582, a_10583),a_10584,CoAP_Option_OSCORE_Option_context( ~M_12048,~M_11516,~M_11518),payload_from_ciphertext( ~M_12047)) = Request(Header(a_10579,a_10580,a_10581, a_10582,a_10583),a_10584,CoAP_Option_OSCORE_Option_context( partial_iv_10589,IDir_10590,idcontext_10588),payload_from_ciphertext( enc_COSE_ciphertext(derive_key_context(MasterSecret_10587, IDir_10590,default_aead_algorithm,idcontext_10588), aead_nonce(IDir_10590,derive_common_iv_context( MasterSecret_10587,idcontext_10588,default_aead_algorithm), partial_iv_10589),(CoAP_POSTCode,payload_10593), AAD(encrypt0_context,encrypt0(oscore_version_one, default_aead_algorithm,IDir_10590,partial_iv_10589))))) |
| ~X_4 = Request(Header(~M_13539,~M_13540,~M_13541,~M_13542, ~M_13543),~M_13535,CoAP_Option_OSCORE_Option_empty, payload_from_ciphertext(~M_13538)) = Request(Header( CoAP_versionOne,CoAP_nonConfirm,CoAP_tokenLength( a_10584),CoAP_CHANGEDCode,responseMessageId_13529), a_10584,CoAP_Option_OSCORE_Option_empty,payload_from_ciphertext( enc_COSE_ciphertext(derive_key_context(MasterSecret_10587, IDri_10586,default_aead_algorithm,idcontext_10588), aead_nonce(IDir_10590,derive_common_iv_context( MasterSecret_10587,idcontext_10588,default_aead_algorithm), partial_iv_10589),(generateResponseCode(CoAP_POSTCode, payload_10593),generateResponsePayload(CoAP_POSTCode, payload_10593)),AAD(encrypt0_context,encrypt0( oscore_version_one,default_aead_algorithm,IDri_10586, partial_iv_10589))))) |

A trace has been found.