

Abbreviations
$\sim X_1$ = Request(Header(a_8765,a_8766,a_8767,a_8768,a_8769), a_8770,CoAP_Option_OSCORE_Option(a_8771, $\sim M_8990$), payload_from_ciphertext(enc_COSE_ciphertext($\sim M_8995$, aad_nonce($\sim M_8990$, $\sim M_8993$,a_8771),(a_8772,a_8773), AAD(oscore_version_one,default_aead_algorithm, $\sim M_8990$,a_8771)))) = Request(Header(a_8765,a_8766, a_8767,a_8768,a_8769),a_8770,CoAP_Option_OSCORE_Option(a_8771,IDir_8775),payload_from_ciphertext(enc_COSE_ciphertext(derive_key(MasterSecret_8776,IDir_8775,default_aead_algorithm), aad_nonce(IDir_8775,derive_common_iv(MasterSecret_8776, default_aead_algorithm),a_8771),(a_8772,a_8773), AAD(oscore_version_one,default_aead_algorithm, IDir_8775,a_8771))))

