JSON Crypto Container 1.0

JSON Crypto Container 1.0

<ietf>draft-hallambaker-json-cryptocontainer

<ipr>trust200902

<category>Standards Track

<area>Security

<version>00

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<organization>Comodo Group Inc.

<email>[philliph@comodo.com](mailto:philliph@comodo.com)

# Abstract

# Introduction

# Examples

## Signed Data Container

{

"JoseWebSignature": {

"unprotected": {

"dig": "S512"},

"payload": "

VGhpcyBpcyBhIHRlc3Q",

"signatures": [{

"protected": "

ewogICJhbGciOiAiUlM1MTIiLAogICJ2YWwiOiAiCm9DalU5MHRnSzZSZXNLazht

a1ozSkEzUEtCb2FreUx4ZzcweThMN1lMc2N0NmNPVmV5OU1taHpQZnRGUGhkYzAK

bU44NEFYNXdQVWZydWZDenZ4RnZhUSJ9",

"signature": "

BjrSvcJ1eZPpPlNIsnmFs1pzoCrRbpmaFpvPcF28Pkg0fIBAQZYqOgngJxyMUJ0Y

veTrybAdKpoLV0vyj6OBZRZLEENH505Wf3qBruuoP2weXXjlPDspjoC892P7430Q

fQR-Dbnis-jB\_qibllJ9BsKPeqk3v-jU8HuKC3BN6vJH7bpEyvpcADZJoHzcu9i0

4F2RCwXi0yXQA1PSch44mcIAYYRfnEH97E4xbtQpl8jo\_aYsnP-t-zDIHX5t4s1c

47fYXyz16Q1a5ZM07hTZ9WO5kNiefPNkI8c10NFSicJuIRLLR-KnFM307yqI347y

KZucs5Kl4A1P0qBhMEQplw"}]}}

Where the contents of Signature are:

{

"alg": "RS512",

"val": "

oCjU90tgK6ResKk8mkZ3JA3PKBoakyLxg70y8L7YLsct6cOVey9MmhzPftFPhdc0

mN84AX5wPUfrufCzvxFvaQ"}

## Encrypted Data Container

{

"JoseWebEncryption": {

"protected": "

ewogICJIZWFkZXIiOiB7CiAgICAiZW5jIjogIkEyNTZDQkMifX0",

"iv": "

8YcOfql72ugnD\_wx6O-7rw",

"recipients": [{

"Header": {

"alg": "RSA-OAEP",

"kid": "MCIND-X7EEM-CVGEB-XQ4EI-K5LOL-FZG52"},

"encrypted\_key": "

VEUCP8kMZOn9kkK9JrQVATZBa7koSyvq4FXjijXsisC9rXsCiTW0etPqU0OSCSrG

BRV8xDK\_eqbJopkVvIUBFRyVONEGsowH16QeTVFNSkbEB89S8Vj8VKmdHoTEgjow

vBxxBb8CGmOnmT8zKnjnHjhy8L8r23whjEDcfk8IGSphYLoO1a-ZI5tzQAXfeGiY

7jLs2iawKilIUrxLBBgzVPA2\_j1V7tlo4q5pM8FV4Ot3z6BrR1Crk6ndIlaDmXHi

J-APZMFZ365IMWb5kyE\_raq8KYnjtRnCA7\_xNKb7aXCbrON5iVrmAgGcTTv\_65Tc

UTCeSXauFxgXazgx8BtU-A"}],

"ciphertext": "

UhM0xiQ0\_m\_TNYJ8S7GpAQ"}}

Where protected is

{

"Header": {

"enc": "A256CBC"}}

## Encrypted and Signed Data Container

{

"JoseWebEncryption": {

"unprotected": {

"dig": "S512"},

"signatures": [{

"protected": "

ewogICJhbGciOiAiUlM1MTIiLAogICJ2YWwiOiAiCjFOZDh2ejFjR2hDTGpJbDhB

ZmswbmpMd0l1M29GR0tBX3Z6QnFzal9VZFhUT2FZUEJVZS1oRG80NXFZazVEcHQK

Q3QtaVhWc2NCN1BCY1FMN3BmM0ZkdyJ9",

"signature": "

SwfqvSpog7Ls79IVWTgNzX68wo3TbfIGt7JI4BqR-2\_t1WwLyIJ0Uw1-2SzU-QiX

\_BeYkM6G-FgGWOGXQGyC\_2Cl8j6z11cCp53LT9KSVVju3FVSTBIHnocxifQWkwnw

7StekKLTasvv3Xm91LmsN9AuLJiMYnxl5EoZIsIaJ9OPdVShxvuu-nBlwT7stW7s

6DwfykxcdxrN1lqXY4qCv6rFfIhouMoAWYUBZ8OcJX1KKQoBlu6h76rE0aTyAOYR

0DXjl9VfGiu6mbpki6WQqOmlOum3plISbtPVoijaAzFtC3dwTi8ho6cnq3aJB\_Pc

kJmkpbbuJwK0Lx4WVHUvzA"}],

"protected": "

ewogICJIZWFkZXIiOiB7CiAgICAiZW5jIjogIkEyNTZDQkMiLAogICAgImRpZyI6

ICJTNTEyIn19",

"iv": "

BPtR-ZfVax3slbKfUcoSZw",

"recipients": [{

"Header": {

"alg": "RSA-OAEP",

"kid": "MDMMX-LV7C6-ZYDFC-3V5T6-73T2C-KEJ43"},

"encrypted\_key": "

C\_mx8xbf\_LcpYe\_S2a7D3bzH0ZApehJVLWxm5tijfuvAj2wFARxL0SHA2yd1LNjO

4jb-F530aGKgqLBQFK7ZH1xsNLa\_x-LGlgutBHpvlGhHcOLjf8gOBpiKfqQQxiMl

vhPl-\_tcuacp7lC6orTW9UsfZ4zyqlU6wI812nR7gNhpK-REDRihIj-Ou6SEgtOq

K7gLjR90p1nX9n62ikahQoMeXOWPhE5OpZDGYPLghrCX-EPE1oAgwfV3Ww9mtJrG

c38vlYUBEYwKFeWxZfKWwdje\_gP4Q3dm73aLULQk80pY\_8x5PSLBZ2T39v9KmLIx

TUnadH3hjJhr8QAf428F4w"}],

"ciphertext": "

D8eQUvZhN5\_lTRFRmkpWmA"}}

Where Protected is

{

"enc": "A256CBC",

"dig": "S512"}

And the signature is

{

"alg": "RS512",

"val": "

1Nd8vz1cGhCLjIl8Afk0njLwIu3oFGKA\_vzBqsj\_UdXTOaYPBUe-hDo45qYk5Dpt

Ct-iXVscB7PBcQL7pf3Fdw"}

# Security Considerations

# IANA Considerations