```
Jose\Object\JWS Object
(
       [is_payload_detached:Jose\Object\JWS:private] => 1
       [encoded_payload:Jose\Object\JWS:private] =>
       [signatures:Jose\Object\JWS:private] => Array
       [payload:Jose\Object\JWS:private] => A JWS with a detached payload
_______
Working with Metadata Statements.
Using examples from: https://openid.andreas.labs.uninett.no
>>>
ey \\ \verb|JhbGci0i]SUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBz0i8vZmVpZGUubm8vIn0.ey \\ \verb|JjbGllbnRfbmFtZSI6IkZvb2RsZSBwb2xscyBhbmQgc3VydmV5cyIsImNvbnRhY|\\ \verb|Sumble of the control of the con
<<<
/home/constantin/public\_html/oidcfed/github/oidcfed\_lib\_php\_rp/examples/jose\_jwt\_jws\_1.php:96: \\
array (size=3)
   0 => string 'eyJhbGci0iJSUzIlNiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBzOi8vZmVpZGUubm8vIn0' (length=71)
   1 => string 'eyJjbGllbnRfbmFtZSI6IkZvb2RsZSBwb2xscyBhbmQgc3VydmV5cyIsImNvbnRhY3RzIjpbImFuZHJlYXMuc29sYmVyZ0B1bmluZXR0Lm5vIiwia29udGFrdEB
   2 => string 'wjM0fZxf0kM88E7Rk1cU74pxZYyqvzpimZijVIC_710G2TUYkD9TV8Zcz1Bl7v9xuANxwSlW29fHk2lK508eDBizwfX4dUJwulnkCJHUcY8hWLpxIJa_o2lXBDX
______
MS Header:
stdClass Object
       [alg] => RS256
        [typ] => JWT
       [kid] => https://feide.no/
MS Payload:
stdClass Object
        [client_name] => Foodle polls and surveys
       [contacts] => Array
              (
                     [0] => andreas.solberg@uninett.no
                     [1] => kontakt@uninett.no
       [redirect_uris] => Array
              (
                     [0] => https://foodl.org/callback
                     [1] => https://www.foodl.org/callback
       [response_types] => Array
              (
                     [0] => code
       [claims] => Array
                     [0] => sub
                     [1] => name
                     [2] => picture
       [iss] => https://feide.no/
       [signing_keys] => Array
              (
                     [0] => stdClass Object
                                   [kty] => RSA
                                   [kid] => https://foodl.org/
                                   [n] => ylWifXilG3JPDx60mj12x8sJsyYoYfKryLtNIT00Gj2wXiQiO4uaPiXMvsFymrNgdpKPkMTiMDndaeVY1cJW45TJD03ld1MVHskUvrADHwA6Jq
                                   [e] => AQAB
              )
       [metadata_statements] => Array
              (
                     [0] => eyJhbGci0iJSUzIINiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBz0i8vZWR1Z2Fpbi5vcmcvIn0.eyJjbGFpbXMi0lsic3ViIiwibmFtZSIsImVtYWlsIi
                     [1] => eyJhbGciOiJSUzIlNiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBzOi8va2FsbWFyLm9yZy8ifQ.eyJjbGFpbXMiOlsic3ViIiwibmFtZSJdLCJpZF90b2t
       [iat] => 1488873238
       [exp] => 1488876838
______
Payload/Claims...
 /home/constantin/public_html/oidcfed/github/oidcfed_lib_php_rp/examples/jose_jwt_jws_1.php:141:
array (size=10)
```

```
'client_name' => string 'Foodle polls and surveys' (length=24)
  'contacts' =>
   array (size=2)
     0 => string 'andreas.solberg@uninett.no' (length=26)
 1 => string 'kontakt@uninett.no' (length=18)
'redirect_uris' =>
   array (size=2)
     0 => string 'https://foodl.org/callback' (length=26)
     1 => string 'https://www.foodl.org/callback' (length=30)
  'response_types' =>
   arrav (size=1)
     0 => string 'code' (length=4)
  'claims' =>
   arrav (size=3)
     0 => string 'sub' (length=3)
1 => string 'name' (length=4)
     2 => string 'picture' (length=7)
  'iss' => string 'https://feide.no/' (length=17)
  'signing_keys' =>
   array (size=1)
     O =>
       array (size=4)
         'kty' => string 'RSA' (length=3)
'kid' => string 'https://foodl.org/' (length=18)
         'n' => string 'ylWifXilG3JPDx60mj12x8sJsyYoYfKryLtNIT00Gj2wXiQi04uaPiXMvsFymrNgdpKPkMTiMDndaeVY1cJW45TJD03ld1MVHskUvrADHwA6JqzKa
         'e' => string 'AQAB' (length=4)
  'metadata_statements' =>
   array (size=2)
     0 => string 'eyJhbGci0iJSUzIINiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBz0i8vZWR1Z2Fpbi5vcmcvIn0.eyJjbGFpbXMi0lsic3ViIiwibmFtZSIsImVtYWlsIiw
     1 => string 'eyJhbGci0iJSUzIINiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBz0i8va2FsbWFyLm9yZy8ifQ.eyJjbGFpbXMi0lsic3ViIiwibmFtZSJdLCJpZF90b2tl
  'iat' => int 1488873238
  'exp' => int 1488876838
______
Signatures count: 1
Signatures:
/home/constantin/public\_html/oidcfed/github/oidcfed\_lib\_php\_rp/examples/jose\_jwt\_jws\_l.php:147: \\
array (size=1)
 0 =
   object(Jose\Object\Signature)[10]
     private 'encoded_protected_headers' => string 'eyJhbGci0iJSUzIINiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBz0i8vZmVpZGUubm8vIn0' (length=71)
     private 'protected_headers' =>
       array (size=3)
         'alg' => string 'RS256' (length=5)
         'typ' => string 'JWT' (length=3)
         'kid' => string 'https://feide.no/' (length=17)
     private 'headers'
       array (size=0)
         empty
     1 s 0 0 0 h 0 N | 0 4 0 /
����T��U饮�-�'.¤2�"@U�♪��ħ;_m�Rø�v∢�]GFMofX���Z��^5�v�L�_yCn[��#�w-���QD�C��ö���������]�7i�' (length=256)
     private 'signature_key' => null
Jose\Object\Signature Object
   [encoded_protected_headers:Jose\Object\Signature:private] => eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6ImhOdHBzOi8vZmVpZGUubm8vIn0
   [protected headers:Jose\Object\Signature:private] => Array
       (
           [alg] => RS256
           [tvp] => JWT
           [kid] => https://feide.no/
   [headers:Jose\Object\Signature:private] => Array
   [signature:Jose\Object\Signature:private] => �34}�_�C<�NŕW♡�qe���:b���T���]₽�5-�?SW�\�Pe��q�⊳q�)V��ŬiJ��∢-����
 8 s���_h�N | ���/
����T��UV�-�'.¤2�"©U�♪0�n4_m�R∅�v≼�]GFMofX���Z��^5�v�L�_yCn[��#�w-���QD�C�ɒö������c]�7i�
   [signature kev:Jose\Object\Signature:private] =>
Protected header(s) (from signature):
Arrav
(
   [0] => Array
       (
           [alg] => RS256
           [typ] => JWT
           [kid] => https://feide.no/
```

```
8/10/2017
```

```
.
Creating JWK for public key for kid: 'kid' => string 'https://feide.no/' (in this example)
@@@@ Instance of JWKInterface @@@@
<#####################################
/home/constantin/public_html/oidcfed/github/oidcfed_lib_php_rp/examples/jose_jwt_jws_1.php:170:
object(Jose\Object\JWK)[13]
  private 'values'
    array (size=4)
      'kty' => string 'RSA' (length=3)
      'kid' => string 'https://feide.no/' (length=17)
      'n' => string '51Fc9aXA576q98xAwrT2rlFmBksT-94Jd_0hlByfP4_K8CuLBTM8HClifdweTFdUdSiB44etC6YLQrJEIyBZ_x-GiEr5oMRNls6HWmWnlBxaDAU16znHQ
      'e' => string 'AQAB' (length=4)
______
Signature verified, below you can see our MS object (JWT/JWS)...
Jose\Object\JWS Object
    [is_payload_detached:Jose\Object\JWS:private] =>
    [encoded_payload:Jose\Object\JWS:private] => eyJjbGllbnRfbmFtZSI6IkZvb2RsZSBwb2xscyBhbmQgc3VydmV5cyIsImNvbnRhY3RzIjpbImFuZHJlYXMuc29s
    [signatures:Jose\Object\JWS:private] => Array
             [0] => Jose\Object\Signature Object
                     [encoded_protected_headers:Jose\Object\Signature:private] => eyJhbGciOiJSUzIINiIsInR5cCI6IkpXVCIsImtpZCI6Imh0dHBzOi8v
                     [protected_headers:Jose\Object\Signature:private] => Array
                              [alg] => RS256
                              [typ] => JWT
                              [kid] => https://feide.no/
                     [headers:Jose\Object\Signature:private] => Array
                     [signature:Jose\0bject\Signature:private] \Rightarrow \diamondsuit34\} \diamondsuit\_ \diamondsuitC < \lozengeN\'(W) \diamondsuit Qe \diamondsuit \diamondsuit \Leftrightarrow :b \diamondsuit \diamondsuit \diamondsuit \top \diamondsuit \diamondsuit \lozenge] \oslash \& \$5 - \diamondsuit ?SW \diamondsuit \land \diamondsuit Pe \diamondsuit \diamondsuit Q \diamondsuit > Q \diamondsuit > Q \diamondsuit > V \diamondsuit \diamondsuit 
 ■ s���_h�N | ���/
����T��U\$�-�'.¤2�''@U�♪0�n5_m�R��v<�]GFMofX���Z��^5�v�L�_yCn[��#�w-���QD�C�ɒö�������c]�7i�
                     [signature_key:Jose\Object\Signature:private] =>
                 )
        )
    [payload:Jose\Object\JWS:private] => Array
             [client_name] => Foodle polls and surveys
             [contacts] => Array
                     [0] => andreas.solberg@uninett.no
                     [1] => kontakt@uninett.no
             [redirect_uris] => Array
                 (
                     [0] => https://foodl.org/callback
                     [1] => https://www.foodl.org/callback
             [response_types] => Array
                 (
                     [0] => code
                 )
             [claims] => Array
                     [0] => sub
                     [1] => name
                     [2] => picture
             [iss] => https://feide.no/
             [signing_keys] => Array
                     [0] => Array
                              [ktv] => RSA
                              [kid] => https://foodl.org/
                              [n] => ylWifXilG3JPDx60mj12x8sJsyYoYfKryLtNIT00Gj2wXiQi04uaPiXMvsFymrNgdpKPkMTiMDndaeVY1cJW45TJD03ld1MVHskUvr
                              [e] => AQAB
```