EMV®

3-D Secure

App-based Cryptographic Worked Samples

Version 2.1.0

August 2018

Legal Notice

This document summarizes EMVCo's present plans for evaluation services and related policies and is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.

Contents

Scope

This document provides worked examples for the various cryptographic functions specified in the *3-D Secure Protocol and Core Functions Specification v2.1.0*. The purpose of this document is to provide input and output values, with intermediate steps where appropriate for the cryptographic mechanisms and algorithms described in the specification.

This document is not an implementation guide, the data elements are constructed (not based on real implementation) and some of the values are random numbers or strings. Steps to derive a cryptographic value could vary based on the technology, tools or frameworks. The steps provided in this document are intended as an illustration and may not represent a production implementation.

Please note this document will not be maintained as new versions of the specification are released to the industry and EMVCo does not plan to address queries that are related to customer implementation and customer specific crypto challenges.

Color coding:

- Plaintext and linking text: Black
- Key Material: Red
- Crypto Output: Green

Note : Elliptic curve keys are shown either as x & y coordinates in base64url format, or as SEC1 point representation (the first byte is 04 followed by the x and the y coordinates) as shown in section 3 of https://tools.ietf.org/html/draft-jivsov-ecc-compact-05.

SDK Encryption of Device Information and DS Decryption—RSA-based Using RSA-OAEP-256 and A128CBC-HS256

Device Information

Plaintext Data

```
{
      "DV":”1.0",
      "DD": {
            "C001":”Android",
            "C002":”HTC One_M8",
            "C004":”5.0.1",
            "C005":”en_US",
            "C006":”Eastern Standard Time",
            "C007":”06797903-fb61-41ed-94c2-4d2b74e27d18",
            "C009":”John's Android Device"
      },
      "DPNA": {
            "C010":”RE01",
            "C011":”RE03"
      },
      "SW": ["SW01", "SW04"]
}
```

Without whitespace

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

In Hex (as will be used later to construct plaintext to be enciphered)

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D346432623734653237643138222C2243303039223A22
4A6F686E277320416E64726F6964204465766963652227D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A2252453033227D2C225357223A5B22
53573031222C2253573034225D7D
```

DS Public Key

from (https://tools.ietf.org/html/rfc7520#page-8 figure 4)

```
{
"kty":     "RSA",
"kid":     "UUIDkeyidentifierforDS",
"use":     "enc",
"n":  "n4EPtAOCc9AlkeQHPzHStgAbgs7bTZLwUBZdR8_KuKPEHLd4rHVTeT-O-
XV2jRojdNhxJWTDvNd7nqQ0VEiZQHz_AJmSCpMaJMRBSFKrKb2wqVwGU_NsYOYL-
QtiWN2lbzcEe6XC0dApr5ydQLrHqkHHig3RBordaZ6Aj-oBHqFEHYpPe7Tpe-
OfVfHd1E6cS6M1FZcD1NNLYD5lFHpPI9bTwJlsde3uhGqC0ZCuEHg8lhzwOHrtIQbS0F
Vbb9k3-
tVTU4fg_3L_vniUFAKwuCLqKnS2BYwdq_mzSnbLY7h_qixoR7jig3__kRhuaxwUkRz5i
aiQkqgc5gHdrNP5zw",
"e":  "AQAB"
}
```

Mødulus *n* in Hex

```
9F810FB4038273D02591E4073F31D2B6001B82CEDB4D92F050165D47CFCAB8A3C41C
B778AC7553793F8EF975768D1A2374D8712564C3BCD77B9EA434544899407CFF0099
920A931A24C4414852AB29BDB0A95C0653F36C60E60BF90B6258DDA56F37047BA5C2
D1D029AF9C9D40BAC7AA41C78A0DD1068ADD699E808FEA011EA1441D8A4F7BB4E97B
E39F55F1DDD44E9C4BA335159703D4D34B603E65147A4F23D6D3C0996C75EDEE846A
82D190AE10783C961CF0387AED2106D2D0555B6FD937FAD5535387E0FF72FFBE7894
1402B0B822EA2A74B6058C1DABF9B34A76CB63B87FAA2C6847B8E2837FFF91186E6B
1C14911CF989A89092A81CE601DDACD3F9CF
```

Exponent *e* in Hex

```
010001
```

Generated Factors

Key (Content Encryption Key and MAC Key) in hex

```
99831FB208244C09B44DBBED945876872A179DB1332508CCC6680B37777CC570
```

The least significant half is the ENC_KEY – in Hex

```
2A179DB1332508CCC6680B37777CC570
```

The most significant half is the MAC_KEY – in Hex

```
99831FB208244C09B44DBBED94587687
```

Initialization Vector (IV) – in Hex

```
C385E0ED5EE632B38BBDC0C2CD1BCA33
```

BASE64url encoded IV

```
w4Xg7V7mMrOLvcDCzRvKMw
```

RSA-OAEP-256 encipherment of the Key

9983… using Modulus 9F81… “n4EP…”; Public Key 010001 “AQAB”] produces:

```
0A997CB4CE5E405369D50AD7CB9706B121CA12937CEF17FA862C53A15D232C22B9FC
3CD4BE993D128281421F308FA0C470D52316F8101DBF076A9167BE48D4F78B5D38DF
58D757E28F15EA3D859C61BD32E4FF1EC5D631967296042C18F946353204469D5ABB
832E122DA455BE32CED77B64ACB77947E8E5302BF20691C54159DB70A6A57C860CD7
1A148644300CFD91A3CD073318BA57302C2F64228AA3DF1AD3022B2BEEACF055A86C
546A9955D1D6E5706AD5C0BE24ABD909BA9EEC108813C6B8F546FE0B76922FC092E1
BD8B82B0B3A658EFAEB1209E65584CDC2F94BF7830B8398294DB13BF304B0695A743
903E2BDC83778C1BA4BEE35E641EE789C54C
```

Base64url encoded

```
Cpl8tM5eQFNp1QrXy5cGsSHKEpN87xf6hixToV0jLCK5_DzUvpk9EoKBQh8wj6DEcNUj
FvgQHb8HapFnvkjU94tdON9Y11fijxXqPYWcYb0y5P8exdYxlnKWBCwY-
UY1MgRGnVq7gy4SLaRVvjLO13tkrLd5R-
jlMCvyBpHFQVnbcKalfIYM1xoUhkQwDP2Ro80HMxi6VzAsL2QiiqPfGtMCKyvurPBVqG
xUaplV0dblcGrVwL4kq9kJup7sEIgTxrj1Rv4LdpIvwJLhvYuCsLOmWO-
usSCeZVhM3C-Uv3gwuDmClNsTvzBLBpWnQ5A-K9yDd4wbpL7jXmQe54nFTA
```

Protected Header

```
{
     "alg":"RSA-OAEP-256",
     "kid":"UUIDkeyidentifierforDS",
     "enc":"A128CBC-HS256"
}
```

Without whitespace

```
{"alg":"RSA-OAEP-256","kid":"UUIDkeyidentifierforDS","enc":"A128CBC-
HS256"}
```

BASE64url encoded

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJraWQiOiJVVUlEa2V5aWRlbnRpZmllcmZvckRT
IiwiZW5jIjoiQTEyOENCQy1IUzI1NiJ9
```

Before encryption plaintext needs padding to 16 byte boundary - using PKCS #7 padding, 4 bytes must be added, so the padded plaintext is:

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D3464326237346532376431382222C2243303039223A22
4A6F686E277320416E64726F6964204465766963652227D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A2252453033227D2C225357223A5B22
53573031222C22535730342255D7D04040404
```

Data Encipherment

CBC encipherment of the plaintext using AES-128 with key “2A17…”; IV “C385…” produces:

```
33A3CD8FBF4D17E656FBF2B3F9F86332886A5655147301EF65D2B80B02AAE660AE63
51709241E950F2946CCA5FE8AE1D55E0A98316859D2E8419EB09EE86F52CE797D27F
EF53552FEB1CE84C1E322186015F29DF34C301CFB23D0C1B92961369083C2356E278
1D59EE71E180A766557D6E49F05AE705EAA4864FE772B17512EF0FF353BB62607B08
7D3C577943A5446E5D96D35BB6A9BDEB338ECE05E191025723C0C30C7B6987D072E7
520C7376FB61BC9100D89D914F34EC6DA01499513031E37A46AAD905AD511D064B91
6AFA9747F3EFA8C1CFDF6535E8B9EA716D2504EDA1D8923F460BC01FBB54578D8A09
6E0098CB0C5865ACF275960745CE13D099A2
```

Base64url encoded

M6PNj79NF-ZW-_Kz-
fhjMohqVlUUcwHvZdK4CwKq5mCuY1FwkkHpUPKUbMpf6K4dVeCpgxaFnS6EGesJ7ob1L
OeX0n_vU1Uv6xzoTB4yIYYBXynfNMMBz7I9DBuSlhNpCDwjVuJ4HVnuceGAp2ZVfW5J8
FrnBeqkhk_ncrF1Eu8P81O7YmB7CH08V3lDpURuXZbTW7apveszjs4F4ZECVyPAwwx7a
YfQcudSDHN2-
2G8kQDYnZFPNOxtoBSZUTAx43pGqtkFrVEdBkuRavqXR_PvqMHP32U16LnqcW0lBO2h2
JI_RgvAH7tUV42KCW4AmMsMWGWs8nWWB0XOE9CZog

Authentication Tag

For the MAC, the Additional Authenticated Data (AAD) is the Protected Header, which as Hex of ASCII of base64url is:

```
“65794A68624763694F694A5355304574543046655433307 94E5459694C434A72615
```

```
“65794A68624763694F694A53555304574543046465543307 94E5459694C434A72615
```

```
“65794A68624763694F694A53555304574543046465543307 94E5459694C434A72615
```

```
“65794A68624763694F694A5355304574543046465543307 94E5459694C434A72615
```

```
“65794A68624763694F694A535553045745430464655433079 4E5459694C434A72615
```

```
“65794A68624763694F694A5355530457454304646554330794E5459694C434A72615
751694F694A5656556C4561325635615752 6C626E52705A6D6C6C636D5A76636B525
```

```
“65794A68624763694F694A5355530457454304646554330794E5459694C434A72615
751694F694A5656556C45613256356157526C626E52705A6D6C6C636D5A76636B525
4496977695A57356A496A6F69515445794F454E4351793149557A49314E694A39”
so the AAD Length (AL) is 0000000000000320 (100 bytes = 800 bits).
```

The data to MAC is the concatenation of AAD (in ASCII), IV, Ciphertext and AL hence the data to MAC in hexadecimal is:

```
65794A68624763694F694A5355530457454304646554330794E5459694C434A726157
51694F694A5656556C45613256356157526C626E52705A6D6C6C636D5A76636B5254
496977695A57356A496A6F69515445794F454E4351793149557A49314E694A39
C385E0ED5EE632B38BBDC0C2CD1BCA33

33A3CD8FBF4D17E656FBF2B3F9F86332886A5655147301EF65D2B80B02AAE660AE63
51709241E950F2946CCA5FE8AE1D55E0A98316859D2E8419EB09EE86F52CE797D27F
EF53552FEB1CE84C1E322186015F29DF34C301CFB23D0C1B92961369083C2356E278
1D59EE71E180A766557D6E49F05AE705EAA4864FE772B17512EF0FF353BB62607B08
7D3C577943A5446E5D96D35BB6A9BDEB338ECE05E191025723C0C30C7B6987D072E7
520C7376FB61BC9100D89D914F34EC6DA01499513031E37A46AAD905AD511D064B91
6AFA9747F3EFA8C1CFDF6535E8B9EA716D2504EDA1D8923F460BC01FBB54578D8A09
6E0098CB0C5865ACF275960745CE13D099A2

0000000000000320
```

MACing using HMAC SHA256 and a key of 9983… produces:

```
29CB6314D4ABB44696D3CDDA4063456A01A52B2E6C6AB238F61B943BB8F24E28
```

The most significant 16 bytes are the authentication tag which is:

```
29CB6314D4ABB44696D3CDDA4063456A
```

Base 64url encoded

```
KctjFNSrtEaW083aQGNFag
```

Resulting JWE looks like:

JWE Protected Header

Encrypted Key

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJraWQiOiJVVUlEa2V5aWRlbnRpZmllcmZvckRT
IiwiZW5jIjoiQTEyOENCQy1IUzI1NiJ9

.

Cpl8tM5eQFNp1QrXy5cGsSHKEpN87xf6hixToV0jLCK5_DzUvpk9EoKBQh8wj6DEcNUj
FvgQHb8HapFnvkjU94tdON9Y11fijxXqPYWcYb0y5P8exdYxlnKWBCwY-
UY1MgRGnVq7gy4SLaRVvjLO13tkrLd5R-
jlMCvyBpHFQVnbcKalfIYM1xoUhkQwDP2Ro80HMxi6VzAsL2QiiqPfGtMCKyvurPBVqG
xUaplV0dblcGrVwL4kq9kJup7sEIgTxrj1Rv4LdpIvwJLhvYuCsLOmWO-
usSCeZVhM3C-Uv3gwuDmClNsTvzBLBpWnQ5A-K9yDd4wbpL7jXmQe54nFTA

.

w4Xg7V7mMrOLvcDCzRvKMw

.

M6PNj79NF-ZW-_Kz-
fhjMohqVlUUcwHvZdK4CwKq5mCuY1FwkkHpUPKUbMpf6K4dVeCpgxaFnS6EGesJ7ob1L
OeX0n_vU1Uv6xzoTB4yIYYBXynfNMMBz7I9DBuSlhNpCDwjVuJ4HVnuceGAp2ZVfW5J8
FrnBeqkhk_ncrF1Eu8P81O7YmB7CH08V3lDpURuXZbTW7apveszjs4F4ZECVyPAwwx7a
YfQcudSDHN2-
2G8kQDYnZFPNOxtoBSZUTAx43pGqtkFrVEdBkuRavqXR_PvqMHP32U16LnqcW0lBO2h2
JI_RgvAH7tUV42KCW4AmMsMWGWs8nWWB0XOE9CZog

.

KctjFNSrtEaW083aQGNFag
```

DS Decryption

Corresponding Private Key d from (https://tools.ietf.org/html/rfc7520#page-8)

Private key d (from RFC)

```
bWUC9B-EFRIo8kpGfh0ZuyGPvMNKvYWNtB_ikiH9k20eT-
O1q_I78eiZkpXxXQ0UTEs2LsNRS-8uJbvQ-
A1irkwMSMkK1J3XTGgdrhCku9gRldY7sNA_AKZGh-Q661_42rINLRCe8W-
nZ34ui_qOfkLnK9QWDDqpaIsA-
bMwWWSDFu2MUBYwkHTMEzLYGqOe04noqeq1hExBTHBOBdkMXiuFhUq1BU6l-
DqEiWxqg82sXt2h-
LMnT3046AOYJoRioz75tSUQfGCshWTBnP5uDjd18kKhyv07lhfSJdrPdM5Plyl21hsFf
4L_mHCuoFau7gdsPfHPxxjVOcOpBrQzwQ
```

In Hex

```
6D6502F41F84151228F24A467E1D19BB218FBCC34ABD858DB41FE29221FD936D1E4F
E3B5ABF23BF1E8999295F15D0D144C4B362EC3514BEF2E25BBD0F80D62AE4C0C48C9
0AD49DD74C681DAE10A4BBD81195D63BB0D03F00A64687E43AEB5FF8DAB20D2D109E
F16FA7677E2E8BFA8E7E42E72BD4160C3AA9688B00F9B33059648316ED8C50163090
74CC1332D81AA39ED389E8A9EAB5844C414C704E05D90C5E2B85854AB5054EA5F83A
84896C6A83CDAC5EDDA1F8B3274F7D38E80398268462A33EF9B525107C60AC8564C1
9CFE6E0E3775F242A1CAFD3B9617D225DACF74CE4F972976D61B057F82FF9870AEA0
56AEEE076C3DF1CFC718D539C3A906B433C1
```

Key Decryption

Decryption of the encrypted key component from JWE using RSA OAEP 256 private key 6D65… “bWUC…”; modulus 9F81… “n4EP…” produces:

```
99831FB208244C09B44DBBED945876872A179DB1332508CCC6680B37777CC570
```

Validation

Validating Authentication Tag component from JWE using HMAC SHA256 with MAC key 9983… MAC of data comprising the concatenation of AAD (as ASCII), IV, Ciphertext and AL. The result is:

```
29CB6314D4ABB44696D3CDDA4063456A01A52B2E6C6AB238F61B943BB8F24E28
```

Converting the first 16 bytes to Base64url format gives

```
KctjFNSrtEaW083aQGNFag
```

Which equals Authentication Tag

Decrypting Ciphertext component from JWE using AES128 CBC with CEK 9983…; IV C385… (PKCS#7 padding removed) **produces**:

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

Device Information BASE64url encoded for AReq to ACS

```
"deviceInfo":"ew0KCSJEViI6ICIxLjAiLA0KCSJERCI6IHsNCgkJIkMwMDEiOiAiQW
5kcm9pZCIsDQoJCSJDMDAyIjogIkhUQyBPbmVfTTgiLA0KCQkiQzAwNCI6ICI1LjAuMS
IsDQoJCSJDMDA1IjogImVuX1VTIiwNCgkJIkMwMDYiOiAiRWFzdGVybiBTdGFuZGFyZC
BUaW1lIiwNCgkJIkMwMDciOiAiMDY3OTc5MDMtZmI2MS00MWVkLTk0YzItNGQyYjc0ZT
I3ZDE4IiwNCgkJIkMwMDkiOiAiSm9obidzIEFuZHJvaWQgRGV2aWNlIg0KCX0sDQoJIk
RQTkEiOiB7DQoJCSJDMDEwIjogIlJFMDEiLA0KCQkiQzAxMSI6ICJSRTAzIg0KCX0sDQ
oJIlNXIjogWyJTVzAxIiwgIlNXMDQiXQ0KfQ0K"
```

SDK Encryption of Device Information and DS Decryption—RSA-based Using RSA-OAEP-256 and A128GCM

Device Information

Plaintext Data

```
{
      "DV":”1.0",
      "DD": {
            "C001":”Android",
            "C002":”HTC One_M8",
            "C004":”5.0.1",
            "C005":”en_US",
            "C006":”Eastern Standard Time",
            "C007":”06797903-fb61-41ed-94c2-4d2b74e27d18",
            "C009":”John's Android Device"
      },
      "DPNA": {
            "C010":”RE01",
            "C011":”RE03"
      },
      "SW": ["SW01", "SW04"]
}
```

Without whitespace

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

In Hex (used later in encipherment)

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D346432623734653237643138222C2243303039223A22
4A6F686E277320416E64726F6964204465766963652227D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A2252453033227D2C225357223A5B22
53573031222C2253573034225D7D
```

DS Public Key

from (https://tools.ietf.org/html/rfc7520#page-8)

```
{
      "kty":"RSA",
      "kid":"UUIDkeyidentifierforDS",
      "use":     "enc",
      "n":"n4EPtAOCc9AlkeQHPzHStgAbgs7bTZLwUBZdR8_KuKPEHLd4rHVTeT-O-
XV2jRojdNhxJWTDvNd7nqQ0VEiZQHz_AJmSCpMaJMRBSFKrKb2wqVwGU_NsYOYL-
QtiWN2lbzcEe6XC0dApr5ydQLrHqkHHig3RBordaZ6Aj-oBHqFEHYpPe7Tpe-
OfVfHd1E6cS6M1FZcD1NNLYD5lFHpPI9bTwJlsde3uhGqC0ZCuEHg8lhzwOHrtIQbS0F
Vbb9k3-
tVTU4fg_3L_vniUFAKwuCLqKnS2BYwdq_mzSnbLY7h_qixoR7jig3__kRhuaxwUkRz5i
aiQkqgc5gHdrNP5zw",
      "e":  "AQAB"
}
```

Modulus *n* in Hex

```
9F810FB4038273D02591E4073F31D2B6001B82CEDB4D92F050165D47CFCAB8A3C41C
B778AC7553793F8EF975768D1A2374D8712564C3BCD77B9EA434544899407CFF0099
920A931A24C4414852AB29BDB0A95C0653F36C60E60BF90B6258DDA56F37047BA5C2
D1D029AF9C9D40BAC7AA41C78A0DD1068ADD699E808FEA011EA1441D8A4F7BB4E97B
E39F55F1DDD44E9C4BA335159703D4D34B603E65147A4F23D6D3C0996C75EDEE846A
82D190AE10783C961CF0387AED2106D2D0555B6FD937FAD5535387E0FF72FFBE7894
1402B0B822EA2A74B6058C1DABF9B34A76CB63B87FAA2C6847B8E2837FFF91186E6B
1C14911CF989A89092A81CE601DDACD3F9CF
```

Exponent *e* in Hex

```
010001
```

Generated Factors

Content Encryption Key (CEK) in hex

```
99831FB208244C09B44DBBED94587687
```

Initialization Vector (IV) – in Hex

```
AD754DB7D24BB8358809955D
```

BASE64url encoded IV

```
rXVNt9JLuDWICZVd
```

RSA-OAEP-256 to encipher the Key

9983… using Modulus 9F81… "n4EP…"; Public Key 010001 "AQAB" produces:

```
9527E1F1D91828DEF1077FE4EACA900D6E68BEB5C5C076CB2BA5A6DEDCEFCAECF89E
EFCCE8733F2F8EBFE9B0BCFF92D7CDFB58C35768EF76116EBCB83F1682FD63886851
66E2BE47AA37A3F85F112A775CE1E6E7A836DE9ED8AB09F3EF7D39D78D51B337D3E6
F89029E2F0A72EA208FA6BBA98B82936767194DF17B162E19B28ED6FED2EC7601D68
7FADB6EF672BD6C5D00224123585E65E8700BB189E0C0416DE03D557F130E3325FEE
B99E2519D9F38EEAA4BDDCF47BF08F454F5BF8B53A205E13B1F6868F3766CA0858E8
38EEBDD86DDE2319993BBEF15FA6ABD94DD5545B0E6542A50B326CCB1A7D8CF6F39F
6E12E100ED0529F3855D3666788DE5C9D9A0
```

Base64url encoded

```
lSfh8dkYKN7xB3_k6sqQDW5ovrXFwHbLK6Wm3tzvyuz4nu_M6HM_L46_6bC8_5LXzftY
w1do73YRbry4PxaC_WOIaFFm4r5Hqjej-
F8RKndc4ebnqDbentirCfPvfTnXjVGzN9Pm-JAp4vCnLqII-
mu6mLgpNnZxlN8XsWLhmyjtb-0ux2AdaH-
ttu9nK9bF0AIkEjWF5l6HALsYngwEFt4D1VfxMOMyX-
65niUZ2fOO6qS93PR78I9FT1v4tTogXhOx9oaPN2bKCFjoOO692G3eIxmZO77xX6ar2U
3VVFsOZUKlCzJsyxp9jPbzn24S4QDtBSnzhV02ZniN5cnZoA
```

Protected Header

```
{
      "alg":”RSA-OAEP-256",
"kid":"UUIDkeyidentifierforDS",
      "enc":”A128GCM"
}
```

Without whitespace

```
{"alg":"RSA-OAEP-
256","kid":"UUIDkeyidentifierforDS","enc":"A128GCM"}
```

BASE64url encoded

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJraWQiOiJVVUlEa2V5aWRlbnRpZmllcmZvckRT
IiwiZW5jIjoiQTEyOEdDTSJ9
```

Data Encipherment

Additional Authenticated Data is ASCII representation of base64url header

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJraWQiOiJVVUlEa2V5aWRlbnRpZmllcmZvckRT
IiwiZW5jIjoiQTEyOEdDTSJ9
```

which is

```
65794A68624763694F694A5355304574543046465543307945459694C434A726157
51694F694A5656556C45613256356157526C626E52705A6D6C6C636D5A76636B5254
496977695A57356A496A6F69515445794F45644454534A39
```

Plaintext is

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D3464326237346532376431382222C2243303039223A22
4A6F686E277320416E64726F696420446576696365227D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A2252453033227D2C225357223A5B22
53573031222C225357303422 5D7D
```

GCM authenticated encryption of the plaintext using AES-128 with key “9983…” and IV “AD75…” produces:

```
A0771E6B60E3471669775254E675ABC118A971EB6B1F8122A5651978FE80BCF224E7
2EEE22C5961B28D60DE6DB747F6834DC2D7BB60124FB16999F378D19AC15895F568D
49808E7554C85F423ED76762E51830FEB13F7D9315401117D9D9AD7EA030CE295454
AE86467D52D27E16C5ECEA8EF3647E4A3EC36AD0A38E124ADEE8747D12946BA100E9
B3A6BED3FFAA34D9E82580DF7EE76BA41E284389B9EBA5E682E53F4266350C02FCCB
8C4EFA9D3BD3B8C8933BE566BD937C9E5B3A7F9B4838EA8C726E54D7F7BCBB533A0A
11F2EB90115C8EAA7C5461FF17295A2025210E251820FD1445F062395A35EBE011AF
B88A7DAC4C36D4A18BA2AF222BF6
```

Base64url encoded

```
oHcea2DjRxZpd1JU5nWrwRipcetrH4EipWUZeP6AvPIk5y7uIsWWGyjWDebbdH9oNNwt
e7YBJPsWmZ83jRmsFYlfVo1JgI51VMhfQj7XZ2LlGDD-sT99kxVAERfZ2a1-
oDDOKVRUroZGfVLSfhbF7OqO82R-
Sj7DatCjjhJK3uh0fRKUa6EA6bOmvtP_qjTZ6CWA337na6QeKEOJueul5oLlP0JmNQwC
_MuMTvqdO9O4yJM75Wa9k3yeWzp_m0g46oxyblTX97y7UzoKEfLrkBFcjqp8VGH_Fyla
ICUhDiUYIP0URfBiOVo16-ARr7iKfaxMNtShi6KvIiv2
```

Authentication Tag

```
BDDB625F0CF465B0A1FB522B4A3A4E9C
```

Base 64url encoded

```
vdtiXwz0ZbCh-1IrSjpOnA
```

Resulting JWE looks like:

JWE Protected Header

Encrypted Key

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJraWQiOiJVVUlEa2V5aWRlbnRpZmllcmZvckRT
IiwiZW5jIjoiQTEyOEdDTSJ9

.

lSfh8dkYKN7xB3_k6sqQDW5ovrXFwHbLK6Wm3tzvyuz4nu_M6HM_L46_6bC8_5LXzftY
w1do73YRbry4PxaC_WOIaFFm4r5Hqjej-
F8RKndc4ebnqDbentirCfPvfTnXjVGzN9Pm-JAp4vCnLqII-
mu6mLgpNnZxlN8XsWLhmyjtb-0ux2AdaH-
ttu9nK9bF0AIkEjWF5l6HALsYngwEFt4D1VfxMOMyX-
65niUZ2fOO6qS93PR78I9FT1v4tTogXhOx9oaPN2bKCFjoOO692G3eIxmZO77xX6ar2U
3VVFsOZUKlCzJsyxp9jPbzn24S4QDtBSnzhV02ZniN5cnZoA

.

rXVNt9JLuDWICZVd

.

oHcea2DjRxZpd1JU5nWrwRipcetrH4EipWUZeP6AvPIk5y7uIsWWGyjWDebbdH9oNNwt
e7YBJPsWmZ83jRmsFYlfVo1JgI51VMhfQj7XZ2LlGDD-sT99kxVAERfZ2a1-
oDDOKVRUroZGfVLSfhbF7OqO82R-
Sj7DatCjjhJK3uh0fRKUa6EA6bOmvtP_qjTZ6CWA337na6QeKEOJueul5oLlP0JmNQwC
_MuMTvqdO9O4yJM75Wa9k3yeWzp_m0g46oxyblTX97y7UzoKEfLrkBFcjqp8VGH_Fyla
ICUhDiUYIP0URfBiOVo16-ARr7iKfaxMNtShi6KvIiv2

.

vdtiXwz0ZbCh-1IrSjpOnA
```

DS Decryption

Corresponding Private Key d from (https://tools.ietf.org/html/rfc7520#page-8)

Private key d

```
bWUC9B-EFRIo8kpGfh0ZuyGPvMNKvYWNtB_ikiH9k20eT-
O1q_I78eiZkpXxXQ0UTEs2LsNRS-8uJbvQ-
A1irkwMSMkK1J3XTGgdrhCku9gRldY7sNA_AKZGh-Q661_42rINLRCe8W-
nZ34ui_qOfkLnK9QWDDqpaIsA-
bMwWWSDFu2MUBYwkHTMEzLYGqOe04noqeq1hExBTHBOBdkMXiuFhUq1BU6l-
DqEiWxqg82sXt2h-
LMnT3046AOYJoRioz75tSUQfGCshWTBnP5uDjd18kKhyv07lhfSJdrPdM5Plyl21hsFf
4L_mHCuoFau7gdsPfHPxxjVOcOpBrQzwQ
```

In Hex

```
6D6502F41F84151228F24A467E1D19BB218FBCC34ABD858DB41FE29221FD936D1E4F
E3B5ABF23BF1E8999295F15D0D144C4B362EC3514BEF2E25BBD0F80D62AE4C0C48C9
0AD49DD74C681DAE10A4BBD81195D63BB0D03F00A64687E43AEB5FF8DAB20D2D109E
F16FA7677E2E8BFA8E7E42E72BD4160C3AA9688B00F9B33059648316ED8C50163090
74CC1332D81AA39ED389E8A9EAB5844C414C704E05D90C5E2B85854AB5054EA5F83A
84896C6A83CDAC5EDDA1F8B3274F7D38E80398268462A33EF9B525107C60AC8564C1
9CFE6E0E3775F242A1CAFD3B9617D225DACF74CE4F972976D61B057F82FF9870AEA0
56AEEE076C3DF1CFC718D539C3A906B433C1
```

Decrypting Encrypted Key component from JWE

using RSA OAEP 256 with private key 6D65…; modulus 9F81… produces:

```
99831FB208244C09B44DBBED94587687
```

Decrypting Ciphertext component from JWE

using AES128 GCM with CEK 9983…; IV AD75… produces:

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

Validation of the Authentication Tag is integral with GCM decryption.

Device Information BASE64url encoded for AReq to ACS

```
"deviceInfo":"ew0KCSJEViI6ICIxLjAiLA0KCSJERCI6IHsNCgkJIkMwMDEiOiAiQW
5kcm9pZCIsDQoJCSJDMDAyIjogIkhUQyBPbmVfTTgiLA0KCQkiQzAwNCI6ICI1LjAuMS
IsDQoJCSJDMDA1IjogImVuX1VTIiwNCgkJIkMwMDYiOiAiRWFzdGVybiBTdGFuZGFyZC
BUaW1lIiwNCgkJIkMwMDciOiAiMDY3OTc5MDMtZmI2MS00MWVkLTk0YzItNGQyYjc0ZT
I3ZDE4IiwNCgkJIkMwMDkiOiAiSm9obidzIEFuZHJvaWQgRGV2aWNlIg0KCX0sDQoJIk
RQTkEiOiB7DQoJCSJDMDEwIjogIlJFMDEiLA0KCQkiQzAxMSI6ICJSRTAzIg0KCX0sDQ
oJIlNXIjogWyJTVzAxIiwgIlNXMDQiXQ0KfQ0K"
```

SDK Encryption of Device Information and DS Decryption—EC-based Using ECDH-ES and A128CBC-HS256

Device Information

Plaintext Data

```
{
      "DV":”1.0",
      "DD": {
            "C001":”Android",
            "C002":”HTC One_M8",
            "C004":”5.0.1",
            "C005":”en_US",
            "C006":”Eastern Standard Time",
            "C007":”06797903-fb61-41ed-94c2-4d2b74e27d18",
            "C009":”John's Android Device"
      },
      "DPNA": {
            "C010":”RE01",
            "C011":”RE03"
      },
      "SW": ["SW01", "SW04"]
}
```

Without whitespace

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

In Hex

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D346432623734653237643138222C2243303039223A22
4A6F686E277320416E64726F696420446576696365227D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A2252453033227D2C225357223A5B22
53573031222C2253573034225D7D
```

DS Public Key (P_{DS})

```
{
"kty":"EC",
"crv":"P-256",
"kid":"UUIDkeyidentifierforDS-EC",
"x":"2_v-MuNZccqwM7PXlakW9oHLP5XyrjMG1UVS8OxYrgA",
"y":"rm1ktLmFIsP2R0YyJGXtsCbaTUesUK31Xc04tHJRolc"
}
```

SDK Ephemeral Key Pair (Q_{SDK}, d_{SDK})

The SDK generated this ephemeral keypair and uses it with the DS public key:

```
{
"kty":"EC",
"crv":"P-256",
"x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4",
"y":"cNToWLSdcFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc",
"d":"iyn--IbkBeNoPu8cN245L6pOQWt2lTH8V0Ds92jQmWA"
}
```

Perform ECDH operation with P_{DS} and d_{SDK}

P_{DS} in SEC1 point representation =

```
04DBFBFE32E35971CAB033B3D795A916F681CB3F95F2AE3306D54552F0EC58AE00AE
6D64B4B98522C3F64746322465EDB026DA4D47AC50ADF55DCD38B47251A257
```

d_{SDK} =

```
8B29FEF886E405E3683EEF1C376E392FAA4E416B769531FC5740ECF768D09960
```

d_{SDK} • Qc in SEC1 point representation =

```
045C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2A6
FB5BD978C1064252DB6F4BA953C018916A9138FB5140FFC2D55A4F7840ECAC
```

Z = x coordinate of above:

```
5C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2
```

Keydatalen = 256 (0x0100) because A128CBC-HS256 requires two 128 bit keys.

There is no apu or apv.

Concat KDF is then used to form the key value as follows:

AlgorithmID = length of 13 + "A128CBC-HS256" = `0000000D 413132384342432D4853323536`

PartyUInfo = length of 0 + null string as there is no apu data: `00000000`

PartyVInfo = length of 0 + null string as there is no apv data: `00000000`

SuppPubInfo = Keydatalen = `00000100`

SuppPrivInfo = empty string

Concatenating 1 + Z + AlgorithmID + PartyUInfo + PartyVInfo + SuppPubInfo + SuppPrivInfo =

```
00000001
5C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2
0000000D 413132384342432D4853323536 00000000 00000000 00000100
```

Hashing the above data with SHA-256 yields this result:

```
4624E920C18D98B2A4F0A87905DEE27E9BC9E1753ED950BBD4B29F986D8695BA
```

This is the CEK

The least significant half is the encryption key

```
9BC9E1753ED950BBD4B29F986D8695BA
```

The most significant half is the authentication key

```
4624E920C18D98B2A4F0A87905DEE27E
```

Initialization Vector - For CBC mode a fresh IV is used. In this example:

```
DE26C1599A2F7BABB2E72223B9AD3239
```

In base64url

```
3ibBWZove6uy5yIjua0yOQ
```

Protected Header

```
{
     "alg":"ECDH-ES",
     "kid":"UUIDkeyidentifierforDS-EC",
     "epk": {
     "kty":"EC",
     "crv":"P-256",
     "x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4",
     “y":"cNToWLSdcFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc"
     },
     "enc":"A128CBC-HS256"
}
```

Without whitespace

{"alg":"ECDH-ES","kid":"UUIDkeyidentifierforDS-EC
","epk":{"kty":"EC","crv":"P-
256","x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4","y":"cNToWLSd
cFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc"},"enc":"A128CBC-HS256"}

BASE64url encoded

eyJhbGciOiJFQ0RILUVTIiwia2lkIjoiVVVJRGtleWlkZW50aWZpZXJmb3JEUy1FQyIs
ImVwayI6eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IkMxUEw0Mmk2a21Oa002
MWF1cEVBZ0xKNGdGMVpSemNWN2xxbzFURzBtTDQiLCJ5IjoiY05Ub1dMU2RjRlFLRy0t
UEdWRVVRcklIUDh3NlRjUnlqMHB5Rng0LVpNYyJ9LCJlbmMiOiJBMTI4Q0JDLUhTMjU2
In0

Before encryption plaintext needs padding to 16 byte boundary - using PKCS #7 padding, 4 bytes must be added, so the padded plaintext is:

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A2245617374657726E2053
74616E646172642054696D65222C2243303037223A22303637393739303332D666236
312D343165642D393463322D3464326237346532376431382222C2243303039223A22
4A6F686E277320416E64726F69642044657669636522 7D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A2252453033227D2C225357223A5B22
53573031222C225357303422 5D7D04040404
```

Data Encipherment

CBC encipherment of the plaintext using AES-128 with key “9BC9…”; IV “DE26….” produces:

```
A9A975B4D436E7F2D0D795C338BB74FC3C2763B55D109D7A86D235F4E9F5CFD46A69
1D06DDD7F0C637D3E9B579C2CF733F1AF2DBD21FC3898D8B75CAE1A51C7A6BAB917B
19F57729C4AF808554DE2E7413B0CD3E2AB8AF857A134BD6FC76BFDC64AA4CF01C7D
30089E59B7616C9AB19BA37EC23C023C2777C518AABD4B75EB1E2F4641D8FC6C28C2
624678532758D70D728B36C89EDD8AD4F1C28AD95AFE669E8B1E1E0E434D25FD06C7
9E44327A4A4D6394A72DFD350C5066ADBD53DECB5F668DC908BED4072F7080263104
72EA9F8A6D8AD9928C89D0BC7EA8F003F26E452E953193CBD80B75DBC96D7C663171
3A0E4E59F15E1F9C54B643838A2C1818B810
```

Base64url encoded:

qal1tNQ25_LQ15XDOLt0_DwnY7VdEJ16htI19On1z9RqaR0G3dfwxjfT6bV5ws9zPxry
29Ifw4mNi3XK4aUcemurkXsZ9XcpxK-AhVTeLnQTsM0-
KrivhXoTS9b8dr_cZKpM8Bx9MAieWbdhbJqxm6N-
wjwCPCd3xRiqvUt16x4vRkHY_GwowmJGeFMnWNcNcos2yJ7ditTxworZWv5mnoseHg5D
TSX9BseeRDJ6Sk1jlKct_TUMUGatvVPey19mjckIvtQHL3CAJjEEcuqfim2K2ZKMidC8
fqjwA_JuRS6VMZPL2At128ltfGYxcToOTlnxXh-cVLZDg4osGBi4EA

Authentication Tag

For the MAC, the Additional Authenticated Data (AAD) is the Protected Header, which in a Hex representation of the base64url string is

```
“65794A68624763694F694A46513052494C5556544969776961326C6B496A6F69565
6564A5247746C65576C6B5A57353061575A705A584A6D62334A4555793146517949
73496D5677617949366579A7264486B694F694A4651794973496D4E7964694936496
C41744D6A55324969776965434936496B4D78554577304D6D6B326132314F6130303
24D5746316345564425A30784B4E4764474D567053656D4E574E327878627A4655527
A4274544451694C434A35496A6F69593035556231644D5532526A526C464C5279307
455456457525656552636B6C49554468334E6C526A556E6C714D484235526E67304C5
6704E59794A394C434A6C626D4D694F694A424D54493451304A444C5568544D6A553
2496E30”
```

so the AAD Length (AL) is 0000000000000898 (275 bytes = 2200 bits).

The data to MAC is the concatenation of AAD (in ASCII), IV, Ciphertext and AL hence the data to MAC in hexadecimal is:

```
65794A68624763694F694A46513052494C5556544969776961326C6B496A6F695656
564A5247746C65576C6B5A57353061575A705A584A6D62334A455579314651794973
496D5677617949366579A7264486B694F694A4651794973496D4E7964694936496C
41744D6A5532496977696543493649B4D78554577304D6D6B326132314F61303032
4D574631634556425A30784B4E4764474D567053656D4E574E327878627A4655527A
4274544451694C434A35496A6F69593035556231644D5532526A526C464C52793074
55456457525656526364B6C49554468334E6C526A556E6C714D484235526E67304C56
704E59794A394C434A6C626D4D694F694A424D54493451304A444C5568544D6A5532
496E30
DE26C1599A2F7BABB2E72223B9AD3239
A9A975B4D436E7F2D0D795C338BB74FC3C2763B55D109D7A86D235F4E9F5CFD46A69
1D06DDD7F0C637D3E9B579C2CF733F1AF2DBD21FC3898D8B75CAE1A51C7A6BAB917B
19F57729C4AF808554DE2E7413B0CD3E2AB8AF857A134BD6FC76BFDC64AA4CF01C7D
30089E59B7616C9AB19BA37EC23C023C2777C518AABD4B75EB1E2F4641D8FC6C28C2
624678532758D70D728B36C89EDD8AD4F1C28AD95AFE669E8B1E1E0E434D25FD06C7
9E44327A4A4D6394A72DFD350C5066ADBD53DECB5F668DC908BED4072F7080263104
72EA9F8A6D8AD9928C89D0BC7EA8F003F26E452E953193CBD80B75DBC96D7C663171
3A0E4E59F15E1F9C54B643838A2C1818B810
0000000000000898
```

MACing using HMAC SHA256 and a key of “4624…” produces:

```
2D4F3D353A5AD03ABFA1950862FD29346C3B13BE62A0C5FD16B1ECB6E1F164DE
```

The most significant 16 bytes are the authentication tag which is

```
2D4F3D353A5AD03ABFA1950862FD2934
```

Base64url encoded

```
LU89NTpa0Dq_oZUIYv0pNA
```

Resulting JWE looks like

JWE Protected Header

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJFQ0RILUVTIiwia2lkIjoiVVVJRGtleWlkZW50aWZpZXJmb3JEUy1FQyIs
ImVwayI6eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IkMxUEw0Mmk2a21Oa002
MWF1cEVBZ0xKNGdGMVpSemNWN2xxbzFURzBtTDQiLCJ5IjoiY05Ub1dMU2RjRlFLRy0t
UEdWRVVRcklIUDh3NlRjUnlqMHB5Rng0LVpNYyJ9LCJlbmMiOiJBMTI4Q0JDLUhTMjU2
In0

.

.

3ibBWZove6uy5yIjua0yOQ

.

qal1tNQ25_LQ15XDOLt0_DwnY7VdEJ16htI19On1z9RqaR0G3dfwxjfT6bV5ws9zPxry
29Ifw4mNi3XK4aUcemurkXsZ9XcpxK-AhVTeLnQTsM0-
KrivhXoTS9b8dr_cZKpM8Bx9MAieWbdhbJqxm6N-
wjwCPCd3xRiqvUt16x4vRkHY_GwowmJGeFMnWNcNcos2yJ7ditTxworZWv5mnoseHg5D
TSX9BseeRDJ6Sk1jlKct_TUMUGatvVPey19mjckIvtQHL3CAJjEEcuqfim2K2ZKMidC8
fqjwA_JuRS6VMZPL2At128ltfGYxcToOTlnxXh-cVLZDg4osGBi4EA

.

LU89NTpa0Dq_oZUIYv0pNA
```

DS Decryption

Decoding the protected header from the message as follows informs the DS of the algorithms and the SDK ephemeral key:

```
{"alg":"ECDH-ES","kid":"UUIDkeyidentifierforDS-
EC","epk":{"kty":"EC","crv":"P-
256","x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4","y":"cNToWLSd
cFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc"},"enc":"A128CBC-HS256"}
```

DS Private Key corresponding to the above public key Q_{DS}

```
dDS = rAZel3KoyQbPejeMRfKzwnqvZfX23fIKek4OKX-5Iu0
```

DS Performs ECDH operation with Q_{SDK} recovered from the protected header and d_{DS}

Q_{SDK} =

```
040B53CBE368BA92636433AD5ABA910080B278805D59473715EE5AA8D531B498BE70
D4E858B49D70540A1BEF8F19511442B2073FCC3A4DC4728F4A72171E3E64C7
```

d_{DS} =

```
AC065E9772A8C906CF7A378C45F2B3C27AAF65F5F6DDF20A7A4E0E297FB922ED
```

$d_{DS} \bullet Q_{SDK}$ =

```
045C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2A6
FB5BD978C1064252DB6F4BA953C018916A9138FB5140FFC2D55A4F7840ECAC
```

Z = x coordinate of above:

```
5C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2
```

This matches the value derived by the SDK as shown above. Using the algorithm from the header, the DS repeats the KDF calculation to yield the same keys.

The SDK then recomputes the authentication key by concatenating the ASCII representation of the base64url encoded protected header, the IV, the ciphertext and the AL and obtains the result:

```
LU89NTpa0Dq_oZUIYv0pNA
```

This matches the value in the header.

Finally the DS deciphers the message yielding the following result:

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

SDK Encryption of Device Information and DS Decryption—EC-based Using ECDH-ES and A128GCM

Device Information

Plaintext Data

```
{
      "DV":"1.0",
      "DD": {
            "C001":"Android",
            "C002":"HTC One_M8",
            "C004":"5.0.1",
            "C005":"en_US",
            "C006":"Eastern Standard Time",
            "C007":"06797903-fb61-41ed-94c2-4d2b74e27d18",
            "C009":"John's Android Device"
      },
      "DPNA": {
            "C010":"RE01",
            "C011":"RE03"
      },
      "SW": ["SW01", "SW04"]
}
```

Without whitespace

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

In Hex

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D346432623734653237643138222C2243303039223A22
4A6F686E277320416E64726F696420446576696365227D2C2244504E41223A7B2243
303130223A225245303122C2243303131223A2252453033227D2C225357223A5B22
53573031222C2253573034225D7D
```

DS Public Key (P_{DS})

```
{
"kty":"EC",
"crv":"P-256",
"x":"2_v-MuNZccqwM7PXlakW9oHLP5XyrjMG1UVS8OxYrgA",
"y":"rm1ktLmFIsP2R0YyJGXtsCbaTUesUK31Xc04tHJRolc"
}
```

SDK Ephemeral Key Pair (Q_{SDK}, d_{SDK})

The SDK generated this ephemeral keypair and uses it with the DS public key:

```
{
"kty":"EC",
"crv":"P-256",
"x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4",
"y":"cNToWLSdcFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc",
"d":"iyn--IbkBeNoPu8cN245L6pOQWt2lTH8V0Ds92jQmWA"
}
```

Perform ECDH operation with P_{DS} and d_{SDK}

P_{DS} in SEC1 point representation =

```
04DBFBFE32E35971CAB033B3D795A916F681CB3F95F2AE3306D54552F0EC58AE00AE
6D64B4B98522C3F64746322465EDB026DA4D47AC50ADF55DCD38B47251A257
```

$\mathrm{d}_{\mathrm{SDK}}$ =

```
8B29FEF886E405E3683EEF1C376E392FAA4E416B769531FC5740ECF768D09960
```

d_{SDK} • Qc in SEC1 point representation =

```
045C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2A6
FB5BD978C1064252DB6F4BA953C018916A9138FB5140FFC2D55A4F7840ECAC
```

Z = x coordinate of above:

```
5C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2
```

Keydatalen = 128 (0x0080) because we need 128 bit key for A128GCM

There is no apu, and apv is the SDK Reference Number.

Concat KDF is then used to form the key value as follows:

AlgorithmID = length of 7 + "A128GCM" = `00000007 4131323847434D`

PartyUInfo = length of 0 + null string as there is no apu data: `00000000`

PartyVInfo = length of 0 + null string as there is no apv data: `00000000`

SuppPubInfo = Keydatalen = `00000080`

SuppPrivInfo = empty string

Concatenating 1 + Z + AlgorithmID + PartyUInfo + PartyVInfo + SuppPubInfo + SuppPrivInfo =

```
00000001
5C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2
00000007 4131323847434D 00000000 00000000 00000080
```

Hashing the above data with SHA-256 yields this result:

```
2D34A7544A68F00500796A9F74FAB25284401D33D0DAD5D955964B97A50BDF2C
```

The most significant half is the encryption key

```
2D34A7544A68F00500796A9F74FAB252
```

Initialization Vector (IV) – in Hex

```
AD754DB7D24BB8358809955D
BASE64url encoded IV
rXVNt9JLuDWICZVd
```

Protected Header

```
{
     "alg":"ECDH-ES",
     "kid":"UUIDkeyidentifierforDS-EC",
     "epk": {
     "kty":"EC",
     "crv":"P-256",
     "x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4",
     “y":"cNToWLSdcFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc"
     },
     "enc":"A128GCM"
}
```

Without whitespace

```
{"alg":"ECDH-ES","kid":"UUIDkeyidentifierforDS-
EC","epk":{"kty":"EC","crv":"P-
256","x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4","y":"cNToWLSd
cFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc"},"enc":"A128GCM"}
```

BASE64url encoded

```
eyJhbGciOiJFQ0RILUVTIiwia2lkIjoiVVVJRGtleWlkZW50aWZpZXJmb3JEUy1FQyIs
ImVwayI6eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IkMxUEw0Mmk2a21Oa002
MWF1cEVBZ0xKNGdGMVpSemNWN2xxbzFURzBtTDQiLCJ5IjoiY05Ub1dMU2RjRlFLRy0t
UEdWRVVRcklIUDh3NlRjUnlqMHB5Rng0LVpNYyJ9LCJlbmMiOiJBMTI4R0NNIn0
```

Data Encipherment

Additional Authenticated Data is ASCII representation of base64url header

```
eyJhbGciOiJFQ0RILUVTIiwia2lkIjoiVVVJRGtleWlkZW50aWZpZXJmb3JEUy1FQyIs
ImVwayI6eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IkMxUEw0Mmk2a21Oa002
MWF1cEVBZ0xKNGdGMVpSemNWN2xxbzFURzBtTDQiLCJ5IjoiY05Ub1dMU2RjRlFLRy0t
UEdWRVVRcklIUDh3NlRjUnlqMHB5Rng0LVpNYyJ9LCJlbmMiOiJBMTI4R0NNIn0
```

which is

```
65794A68624763694F694A46513052494C5556544969776961326C6B496A6F695656
564A5247746C65576C6B5A57353061575A705A584A6D62334A455579314651794973
496D56776179493665794A7264486B694F694A4651794973496D4E7964694936496C
41744D6A553249697769654349364B4D78554577304D6D6B326132314F61303032
4D5746316345564425A30784B4E4764474D567053656D4E574E327878627A4655527A
4274544451694C434A35496A6F695930355556231644D5532526A526C464C52793074
55456457525656652636B6C49554468334E6C526A556E6C714D484235526E67304C56
704E59794A394C434A6C626D4D694F694A424D54493452304E4E496E30
```

Plaintext is

```
7B224456223A22312E30222C224444223A7B2243303031223A22416E64726F696422
2C2243303032223A22485443204F6E655F4D38222C2243303034223A22352E302E31
222C2243303035223A22656E5F5553222C2243303036223A224561737465726E2053
74616E646172642054696D65222C2243303037223A2230363739373930332D666236
312D343165642D393463322D3464326237346532376431382222C2243303039223A22
4A6F686E277320416E64726F6964204465766963652227D2C2244504E41223A7B2243
303130223A2252453031222C2243303131223A22524530332227D2C225357223A5B22
53573031222C2253573034225D7D
```

GCM authenticated encryption of the plaintext using AES-128 with key ”2D34…” and “IV AD75…” produces:

```
E428C13C2F8E719DAEE08D382F987E5EDCBD506E47AF8E3BBD2AC8732805B5C63746
04602AADAF5CA076650C6B38032C909C8D016074AE6B2B691FA7B88FFD465AE461FC
571B2851D44F7A2A0A4F9FF5AEEAA2937056392798E770AF7FF791D7CE2CFA6FE5C2
515E92AA71608239392C083F1AB281025F5BF6BB4B19E0EDEA01A68FBDD11C184138
B11FF3D0AD382F6B416DB41005E053EB4DAFC0D5B1CB07CDF5820DBEFE9874D20538
BD5A83FB17D054EF4D8DCFEF8A6C70AABD078FEFEB14D60769348C42699B1460812E
2C573B801BAC93E04FCD4932E984944A9D415823DE7ECE02DE03DC8A11B6B556E403
E330D6CCD7ECBDE50BA033D32B06
```

Base64url encoded

5CjBPC-OcZ2u4I04L5h-
Xty9UG5Hr447vSrIcygFtcY3RgRgKq2vXKB2ZQxrOAMskJyNAWB0rmsraR-
nuI_9RlrkYfxXGyhR1E96KgpPn_Wu6qKTcFY5J5jncK9_95HXziz6b-
XCUV6SqnFggjk5LAg_GrKBAl9b9rtLGeDt6gGmj73RHBhBOLEf89CtOC9rQW20EAXgU-
tNr8DVscsHzfWCDb7-mHTSBTi9WoP7F9BU702Nz--KbHCqvQeP7-
sU1gdpNIxCaZsUYIEuLFc7gBusk-BPzUky6YSUSp1BWCPefs4C3gPcihG2tVbkA-
Mw1szX7L3lC6Az0ysG

And Authentication Tag

```
0F48F1098641F2C008FFDBDC9E91BB53
```

Base 64url encoded

```
D0jxCYZB8sAI_9vcnpG7Uw
```

Resulting JWE looks like:

JWE Protected Header

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJFQ0RILUVTIiwia2lkIjoiVVVJRGtleWlkZW50aWZpZXJmb3JEUy1FQyIs
ImVwayI6eyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IkMxUEw0Mmk2a21Oa002
MWF1cEVBZ0xKNGdGMVpSemNWN2xxbzFURzBtTDQiLCJ5IjoiY05Ub1dMU2RjRlFLRy0t
UEdWRVVRcklIUDh3NlRjUnlqMHB5Rng0LVpNYyJ9LCJlbmMiOiJBMTI4R0NNIn0

.

.

rXVNt9JLuDWICZVd

.

5CjBPC-OcZ2u4I04L5h-
Xty9UG5Hr447vSrIcygFtcY3RgRgKq2vXKB2ZQxrOAMskJyNAWB0rmsraR-
nuI_9RlrkYfxXGyhR1E96KgpPn_Wu6qKTcFY5J5jncK9_95HXziz6b-
XCUV6SqnFggjk5LAg_GrKBAl9b9rtLGeDt6gGmj73RHBhBOLEf89CtOC9rQW20EAXgU-
tNr8DVscsHzfWCDb7-mHTSBTi9WoP7F9BU702Nz--KbHCqvQeP7-
sU1gdpNIxCaZsUYIEuLFc7gBusk-BPzUky6YSUSp1BWCPefs4C3gPcihG2tVbkA-
Mw1szX7L3lC6Az0ysG

.

D0jxCYZB8sAI_9vcnpG7Uw
```

DS Decryption

The DS unpacks the protected header thus

```
{"alg":"ECDH-ES","kid":"UUIDkeyidentifierforDS-
EC","epk":{"kty":"EC","crv":"P-
256","x":"C1PL42i6kmNkM61aupEAgLJ4gF1ZRzcV7lqo1TG0mL4","y":"cNToWLSd
cFQKG--PGVEUQrIHP8w6TcRyj0pyFx4-ZMc"},"enc":"A128GCM"}
```

From this it determines the algorithms and the ephemeral public key of the SDK

DS Private Key corresponding to the above public key Q_{DS}

d_{DS} = `rAZel3KoyQbPejeMRfKzwnqvZfX23fIKek4OKX-5Iu0`

DS Performs ECDH operation with Q_{SDK} recovered from the protected header and d_{DS}

Q_{SDK} in SEC1 point representation =

```
040B53CBE368BA92636433AD5ABA910080B278805D59473715EE5AA8D531B498BE70
D4E858B49D70540A1BEF8F19511442B2073FCC3A4DC4728F4A72171E3E64C7
```

d_{DS} =

```
AC065E9772A8C906CF7A378C45F2B3C27AAF65F5F6DDF20A7A4E0E297FB922ED
```

$d_{DS} \bullet Q_{SDK}$ in SEC1 point representation =

```
045C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2A6
FB5BD978C1064252DB6F4BA953C018916A9138FB5140FFC2D55A4F7840ECAC
```

Z = x coordinate of above:

```
5C32BC13F8ECEB148ABAF2A6B9DD1F6891BB2A80AB09347C64068231A59E8CA2
```

This matches the value derived by the SDK as shown above. Using the algorithm from the header, the DS repeats the KDF calculation to yield the same key `2D34A7544A68F00500796A9F74FAB252`.

Using the ASCII representation of the base64url coded protected header, the IV of `rXVNt9JLuDWICZVd` and the token `D0jxCYZB8sAI_9vcnpG7Uw` the ACS deciphers and validates the ciphertext yielding the following result:

```
{"DV":"1.0","DD":{"C001":"Android","C002":"HTC
One_M8","C004":"5.0.1","C005":"en_US","C006":"Eastern Standard
Time","C007":"06797903-fb61-41ed-94c2-4d2b74e27d18","C009":"John's
Android
Device"},"DPNA":{"C010":"RE01","C011":"RE03"},"SW":["SW01","SW04"]}
```

ACS Signed Content and SDK Validation—RSA-based Using PS256

Note: PS256 uses random data to generate the signature - it might not be possible to exactly replicate the results in this example.

Payload to be signed

```
{
“ACS Ephemeral Public Key (QT)”:{
"kty":"EC",
"crv":"P-256",
"x":"mPUKT_bAWGHIhg0TpjjqVsP1rXWQu_vwVOHHtNkdYoA",
"y":"8BQAsImGeAS46fyWw5MhYfGTT0IjBpFw2SS34Dv4Irs",
},
“SDK Ephemeral Public Key (QC)”:{
"kty":"EC",
"crv":"P-256",
"x":"Ze2loSV3wrroKUN_4zhwGhCqo3Xhu1td4QjeQ5wIVR0",
"y":"HlLtdXARY_f55A3fnzQbPcm6hgr34Mp8p-nuzQCE0Zw",
},
“ACS URL”:”http://acsserver.domainname.com”
}
```

Without whitespace

```
{“ACS Ephemeral Public Key (QT)”:{"kty":"EC","crv":"P-
256","x":"mPUKT_bAWGHIhg0TpjjqVsP1rXWQu_vwVOHHtNkdYoA","y":"8BQAsImG
eAS46fyWw5MhfGTT0IjBpFw2SS34Dv4Irs",},“SDK Ephemeral Public Key
(QC)”:{"kty":"EC","crv":"P-
256","x":"Ze2loSV3wrroKUN_4zhwGhCqo3Xhu1td4QjeQ5wIVR0","y":"HlLtdXAR
Y_f55A3fnzQbPcm6hgr34Mp8p-nuzQCE0Zw",},“ACS
URL”:”http://acsserver.domainname.com”}
```

BASE64url encoded

```
eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ
```

ACS RSA Private Key – 2048 bits

```
{
"kty":"RSA",
"use":"sig",
"n":"kNrPIBDXMU6fcyv5i-QHQAQ-K8gsC3HJb7FYhYaw8hXbNJa-t8q0lD
KwLZgQXYV-ffWxXJv5GGrlZE4GU52lfMEegTDzYTrRQ3tepgKFjMGg6I
y6fkl1ZNsx2gEonsnlShfzA9GJwRTmtKPbk1s-hwx1IU5AT-AIelNqBg
cF2vE5W25_SGGBoaROVdUYxqETDggM1z5cKV4ZjDZ8-lh4oVB07bkac6
LQdHpJUUySH_Er20DXx30Kyi97PciXKTS-QKXnmm8ivyRCmux22ZoPUi
nd2BKC5OiG4MwALhaL2Z2k8CsRdfy-7dg7z41Rp6D0ZeEvtaUp4bX4aK
raL4rTfw",
"e":"AQAB",
"d":"ZLe_TIxpE9-W_n2VBa-HWvuYPtjvxwVXClJFOpJsdea8g9RMx34qEO
EtnoYc2un3CZ3LtJi-mju5RAT8YSc76YJds3ZVw0UiO8mMBeG6-iOnvg
obobNx7K57-xjTJZU72EjOr9kB7z6ZKwDDq7HFyCDhUEcYcHFVc7iL_6
TibVhAhOFONWlqlJgEgwVYd0rybNGKifdnpEbwyHoMwY6HM1qvnEFgP7
iZ0YzHUT535x6jj4VKcdA7ZduFkhUauysySEW7mxZM6fj1vdjJIy9LD1
fIz30Xv4ckoqhKF5GONU6tNmMmNgAD6gIViyEle1PrIxl1tBhCI14bRW
zrpHgAQ",
}
```

Private key *d* In Hex

```
64B7BF4C8C6913DF96FE7D9505AF875AFB983ED8EFC705570A52453A926C75E6BC83
D44CC77E2A10E12D9E861CDAE9F7099DCBB498BE9A3BB94404FC61273BE9825DB376
55C345223BC98C05E1BAFA23A7BE0A1BA1B371ECAE7BFB18D325953BD848CEAFD901
EF3E992B00C3ABB1C5C820E150471870715573B88BFFA4E26D584084E14E35696A94
9804830558774AF26CD18A89F767A446F0C87A0CC18E87335AAF9C41603FB899D18C
C7513E77E71EA38F854A71D03B65DB8592151ABB2B324845BB9B164CE9F8F5BDD8C9
232F4B0F57C8CF7D17BF8724A2A84A17918E354EAD366326360003EA02158B21257B
53EB231975B41842235E1B456FB3AE91E001
```

Modulus *n* in Hex

```
90DACF2010D7314E9F732BF98BE40740043E2BC82C0B71C96FB1588586B0F215DB34
96BEB7CAB49432B02D98105D857E7DF5B15C9BF9186AE5644E06539DA57CC11E8130
F3613AD1437B5EA602858CC1A0E88CBA7E497564DB31DA01289EC9E54A17F303D189
C114E6B4A3DB935B3E870C75214E404FE0087A536A060705DAF1395B6E7F486181A1
A44E55D518C6A1130E080CD73E5C295E198C367CFA5878A15074EDB91A73A2D0747A
49514C921FF12BDB40D7C77D0ACA2F7B3DC8972934BE40A5E79A6F22BF24429AEC76
D99A0F5229DDD81282E4E886E0CC002E168BD99DA4F02B1175FCBEEDD83BCF8D51A7
A0F465E12FB5A529E1B5F868AADA2F8AD37F
```

The ACS possesses a DS generated X.509 certificate for its RSA signature key:

```
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WDANBgkqhkiG9w0BAQsFADBH
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHZXhhbXBsZTEX
MBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTE1NDAyWhcNMjcxMjMx
MTMzMDAwWjBIMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYH
ZXhhbXBsZTEYMBYGA1UEAwwPUlNBIEV4YW1wbGUgQUNTMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkNrPIBDXMU6fcyv5i+QHQAQ+K8gsC3HJb7FYhYaw
8hXbNJa+t8q0lDKwLZgQXYV+ffWxXJv5GGrlZE4GU52lfMEegTDzYTrRQ3tepgKF
jMGg6Iy6fkl1ZNsx2gEonsnlShfzA9GJwRTmtKPbk1s+hwx1IU5AT+AIelNqBgcF
2vE5W25/SGGBoaROVdUYxqETDggM1z5cKV4ZjDZ8+lh4oVB07bkac6LQdHpJUUyS
H/Er20DXx30Kyi97PciXKTS+QKXnmm8ivyRCmux22ZoPUind2BKC5OiG4MwALhaL
2Z2k8CsRdfy+7dg7z41Rp6D0ZeEvtaUp4bX4aKraL4rTfwIDAQABo2AwXjAMBgNV
HRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDAdBgNVHQ4EFgQUktwf6ZpTCxjYKw/B
LW6PeiNX4swwHwYDVR0jBBgwFoAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZI
hvcNAQELBQADggEBAGuNHxv/BR6j7lCPysm1uhrbjBOqdrhJMR/Id4dB2GtdEScl
3irGPmXyQ2SncTWhNfsgsKDZWp5Bk7+Otnty0eNUMk3hZEqgYjxhzau048XHbsfG
voJaMGZZNTwUvTUz2hkkhgpx9yQAKIA2LzFKcgYhelPu4GW5rtEuxu3IS6WYy3D1
GtF3naEWkjUra8hQOhOl2S+CYHmRd6lGkXykVDajMgd2AJFzXdKLxTt0OYrWDGlU
SzGACRBCd5xbRmATIldtccaGqDN1cNWv0I/bPN8EpKS6B0WaZcPasItKWpDC85Jw
1GrDxdhwoKHoxtSG+odiTwB5zLbrn2OsRE5bV7E=
-----END CERTIFICATE-----
```

This certificate may be parsed as follows:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6d:2e:02:e0:14:a2:83:bb:ae:27:9b:83:a5:e4:f8:58
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=example, CN=RSA Example DS
        Validity
            Not Before: Nov 21 11:54:02 2017 GMT
            Not After : Dec 31 13:30:00 2027 GMT
        Subject: DC=com, DC=example, CN=RSA Example ACS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:90:da:cf:20:10:d7:31:4e:9f:73:2b:f9:8b:e4:
                    07:40:04:3e:2b:c8:2c:0b:71:c9:6f:b1:58:85:86:
                    b0:f2:15:db:34:96:be:b7:ca:b4:94:32:b0:2d:98:
                    10:5d:85:7e:7d:f5:b1:5c:9b:f9:18:6a:e5:64:4e:
                    06:53:9d:a5:7c:c1:1e:81:30:f3:61:3a:d1:43:7b:
                    5e:a6:02:85:8c:c1:a0:e8:8c:ba:7e:49:75:64:db:
                    31:da:01:28:9e:c9:e5:4a:17:f3:03:d1:89:c1:14:
                    e6:b4:a3:db:93:5b:3e:87:0c:75:21:4e:40:4f:e0:
                    08:7a:53:6a:06:07:05:da:f1:39:5b:6e:7f:48:61:
                    81:a1:a4:4e:55:d5:18:c6:a1:13:0e:08:0c:d7:3e:
                    5c:29:5e:19:8c:36:7c:fa:58:78:a1:50:74:ed:b9:
                    1a:73:a2:d0:74:7a:49:51:4c:92:1f:f1:2b:db:40:
                    d7:c7:7d:0a:ca:2f:7b:3d:c8:97:29:34:be:40:a5:
                    e7:9a:6f:22:bf:24:42:9a:ec:76:d9:9a:0f:52:29:
                    dd:d8:12:82:e4:e8:86:e0:cc:00:2e:16:8b:d9:9d:
```

```
                    a4:f0:2b:11:75:fc:be:ed:d8:3b:cf:8d:51:a7:a0:
                    f4:65:e1:2f:b5:a5:29:e1:b5:f8:68:aa:da:2f:8a:
                    d3:7f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Subject Key Identifier:

92:DC:1F:E9:9A:53:0B:18:D8:2B:0F:C1:2D:6E:8F:7A:23:57:E2:CC
            X509v3 Authority Key Identifier:

keyid:C3:83:02:9D:BC:03:EA:6D:B0:A6:7A:10:DA:C3:43:F0:6A:F2:3C:DE

    Signature Algorithm: sha256WithRSAEncryption
         6b:8d:1f:1b:ff:05:1e:a3:ee:50:8f:ca:c9:b5:ba:1a:db:8c:
         13:aa:76:b8:49:31:1f:c8:77:87:41:d8:6b:5d:11:27:25:de:
         2a:c6:3e:65:f2:43:64:a7:71:35:a1:35:fb:20:b0:a0:d9:5a:
         9e:41:93:bf:8e:b6:7b:72:d1:e3:54:32:4d:e1:64:4a:a0:62:
         3c:61:cd:ab:b4:e3:c5:c7:6e:c7:c6:be:82:5a:30:66:59:35:
         3c:14:bd:35:33:da:19:24:86:0a:71:f7:24:00:28:80:36:2f:
         31:4a:72:06:21:7a:53:ee:e0:65:b9:ae:d1:2e:c6:ed:c8:4b:
         a5:98:cb:70:f5:1a:d1:77:9d:a1:16:92:35:2b:6b:c8:50:3a:
         13:a5:d9:2f:82:60:79:91:77:a9:46:91:7c:a4:54:36:a3:32:
         07:76:00:91:73:5d:d2:8b:c5:3b:74:39:8a:d6:0c:69:54:4b:
         31:80:09:10:42:77:9c:5b:46:60:13:22:57:6d:71:c6:86:a8:
         33:75:70:d5:af:d0:8f:db:3c:df:04:a4:a4:ba:07:45:9a:65:
         c3:da:b0:8b:4a:5a:90:c2:f3:92:70:d4:6a:c3:c5:d8:70:a0:
         a1:e8:c6:d4:86:fa:87:62:4f:00:79:cc:b6:eb:9f:63:ac:44:
         4e:5b:57:b1
```

It provides a copy for the SDK in the protected header along with the description of the algorithm that the ACS will use to sign the payload thus:

Protected Header

```
{
“alg”:”PS256”,
“x5c”:
[“MIIDeTCCAmGgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WDANBgkqhkiG9w0BAQsFADBH
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHZXhhbXBsZTEX
MBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTE1NDAyWhcNMjcxMjMx
MTMzMDAwWjBIMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYH
ZXhhbXBsZTEYMBYGA1UEAwwPUlNBIEV4YW1wbGUgQUNTMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAkNrPIBDXMU6fcyv5i+QHQAQ+K8gsC3HJb7FYhYaw
8hXbNJa+t8q0lDKwLZgQXYV+ffWxXJv5GGrlZE4GU52lfMEegTDzYTrRQ3tepgKF
jMGg6Iy6fkl1ZNsx2gEonsnlShfzA9GJwRTmtKPbk1s+hwx1IU5AT+AIelNqBgcF
2vE5W25/SGGBoaROVdUYxqETDggM1z5cKV4ZjDZ8+lh4oVB07bkac6LQdHpJUUyS
H/Er20DXx30Kyi97PciXKTS+QKXnmm8ivyRCmux22ZoPUind2BKC5OiG4MwALhaL
2Z2k8CsRdfy+7dg7z41Rp6D0ZeEvtaUp4bX4aKraL4rTfwIDAQABo2AwXjAMBgNV
HRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIHgDAdBgNVHQ4EFgQUktwf6ZpTCxjYKw/B
LW6PeiNX4swwHwYDVR0jBBgwFoAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZI
hvcNAQELBQADggEBAGuNHxv/BR6j7lCPysm1uhrbjBOqdrhJMR/Id4dB2GtdEScl
3irGPmXyQ2SncTWhNfsgsKDZWp5Bk7+Otnty0eNUMk3hZEqgYjxhzau048XHbsfG
voJaMGZZNTwUvTUz2hkkhgpx9yQAKIA2LzFKcgYhelPu4GW5rtEuxu3IS6WYy3D1
GtF3naEWkjUra8hQOhOl2S+CYHmRd6lGkXykVDajMgd2AJFzXdKLxTt0OYrWDGlU
SzGACRBCd5xbRmATIldtccaGqDN1cNWv0I/bPN8EpKS6B0WaZcPasItKWpDC85Jw
1GrDxdhwoKHoxtSG+odiTwB5zLbrn2OsRE5bV7E=”]
}
```

Note: in continued deference to consistency in the RFCs, the cert is base64 not base64url.

Without whitespace

```
{"alg":"PS256","x5c":["MIIDeTCCAmGgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WDANB
gkqhkiG9w0BAQsFADBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBG
RYHZXhhbXBsZTEXMBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTE1NDAyW
hcNMjcxMjMxMTMzMDAwWjBIMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyL
GQBGRYHZXhhbXBsZTEYMBYGA1UEAwwPUlNBIEV4YW1wbGUgQUNTMIIBIjANBgkqhkiG9
w0BAQEFAAOCAQ8AMIIBCgKCAQEAkNrPIBDXMU6fcyv5i+QHQAQ+K8gsC3HJb7FYhYaw8
hXbNJa+t8q0lDKwLZgQXYV+ffWxXJv5GGrlZE4GU52lfMEegTDzYTrRQ3tepgKFjMGg6
Iy6fkl1ZNsx2gEonsnlShfzA9GJwRTmtKPbk1s+hwx1IU5AT+AIelNqBgcF2vE5W25/S
GGBoaROVdUYxqETDggM1z5cKV4ZjDZ8+lh4oVB07bkac6LQdHpJUUySH/Er20DXx30Ky
i97PciXKTS+QKXnmm8ivyRCmux22ZoPUind2BKC5OiG4MwALhaL2Z2k8CsRdfy+7dg7z
41Rp6D0ZeEvtaUp4bX4aKraL4rTfwIDAQABo2AwXjAMBgNVHRMBAf8EAjAAMA4GA1UdD
wEB/wQEAwIHgDAdBgNVHQ4EFgQUktwf6ZpTCxjYKw/BLW6PeiNX4swwHwYDVR0jBBgwF
oAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZIhvcNAQELBQADggEBAGuNHxv/BR6j7
lCPysm1uhrbjBOqdrhJMR/Id4dB2GtdEScl3irGPmXyQ2SncTWhNfsgsKDZWp5Bk7+Ot
nty0eNUMk3hZEqgYjxhzau048XHbsfGvoJaMGZZNTwUvTUz2hkkhgpx9yQAKIA2LzFKc
gYhelPu4GW5rtEuxu3IS6WYy3D1GtF3naEWkjUra8hQOhOl2S+CYHmRd6lGkXykVDajM
gd2AJFzXdKLxTt0OYrWDGlUSzGACRBCd5xbRmATIldtccaGqDN1cNWv0I/bPN8EpKS6B
0WaZcPasItKWpDC85Jw1GrDxdhwoKHoxtSG+odiTwB5zLbrn2OsRE5bV7E="]}
```

BASE64url encoded

```
eyJhbGciOiJQUzI1NiIsIng1YyI6WyJNSUlEZVRDQ0FtR2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V0RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSk13SGhjTk1UY3hNVEl4TVRFMU5EQXlX
aGNOTWpjeE1qTXhNVE16TURBd1dqQklNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVZTUJZR0ExVUVBd3dQVWxO
QklFVjRZVzF3YkdVZ1FVTlRNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1J
SUJDZ0tDQVFFQWtOclBJQkRYTVU2ZmN5djVpK1FIUUFRK0s4Z3NDM0hKYjdGWWhZYXc4
aFhiTkphK3Q4cTBsREt3TFpnUVhZVitmZld4WEp2NUdHcmxaRTRHVTUybGZNRWVnVER6
WVRyUlEzdGVwZ0tGak1HZzZJeTZma2wxWk5zeDJnRW9uc25sU2hmekE5R0p3UlRtdEtQ
Ymsxcytod3gxSVU1QVQrQUllbE5xQmdjRjJ2RTVXMjUvU0dHQm9hUk9WZFVZeHFFVERn
Z00xejVjS1Y0WmpEWjgrbGg0b1ZCMDdia2FjNkxRZEhwSlVVeVNIL0VyMjBEWHgzMEt5
aTk3UGNpWEtUUytRS1hubW04aXZ5UkNtdXgyMlpvUFVpbmQyQktDNU9pRzRNd0FMaGFM
MloyazhDc1JkZnkrN2RnN3o0MVJwNkQwWmVFdnRhVXA0Ylg0YUtyYUw0clRmd0lEQVFB
Qm8yQXdYakFNQmdOVkhSTUJBZjhFQWpBQU1BNEdBMVVkRHdFQi93UUVBd0lIZ0RBZEJn
TlZIUTRFRmdRVWt0d2Y2WnBUQ3hqWUt3L0JMVzZQZWlOWDRzd3dId1lEVlIwakJCZ3dG
b0FVdzRNQ25id0Q2bTJ3cG5vUTJzTkQ4R3J5UE40d0RRWUpLb1pJaHZjTkFRRUxCUUFE
Z2dFQkFHdU5IeHYvQlI2ajdsQ1B5c20xdWhyYmpCT3FkcmhKTVIvSWQ0ZEIyR3RkRVNj
bDNpckdQbVh5UTJTbmNUV2hOZnNnc0tEWldwNUJrNytPdG50eTBlTlVNazNoWkVxZ1lq
eGh6YXUwNDhYSGJzZkd2b0phTUdaWk5Ud1V2VFV6Mmhra2hncHg5eVFBS0lBMkx6Rktj
Z1loZWxQdTRHVzVydEV1eHUzSVM2V1l5M0QxR3RGM25hRVdralVyYThoUU9oT2wyUytD
WUhtUmQ2bEdrWHlrVkRhak1nZDJBSkZ6WGRLTHhUdDBPWXJXREdsVVN6R0FDUkJDZDV4
YlJtQVRJbGR0Y2NhR3FETjFjTld2MEkvYlBOOEVwS1M2QjBXYVpjUGFzSXRLV3BEQzg1
SncxR3JEeGRod29LSG94dFNHK29kaVR3QjV6TGJybjJPc1JFNWJWN0U9Il19
```

Message to be signed: Protected header and Payload with a ‘.’ Separator.

(Whitespace omitted).

```
eyJhbGciOiJQUzI1NiIsIng1YyI6WyJNSUlEZVRDQ0FtR2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V0RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSRk13SGhjTk1UY3hNVEl4TVRFMU5EQXlX
aGNOTWpjeE1qTXhNVE16TURBd1dqQklNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVZTUJZR0ExVUVBd3dQVWxO
QklFVjRZVzF3YkdVZ1FVTlRNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1J
SUJDZ0tDQVFFQWtOclBJQkRYTVU2ZmN5djVpK1FIUUFRK0s4Z3NDM0hKYjdGWWhZYXc4
aFhiTkphK3Q4cTBsREt3TFpnUVhZVitmZld4WEp2NUdHcmxaRTRHVTUybGZNRWVnVER6
WVRyUlEzdGVwZ0tGak1HZzZJeTZma2wxWk5zeDJnRW9uc25sU2hmekE5R0p3UlRtdEtQ
Ymsxcytod3gxSVU1QVQrQUllbE5xQmdjRjJ2RTVXMjUvU0dHQm9hUk9WZFVZeHFFVERn
Z00xejVjS1Y0WmpEWjgrbGg0b1ZCMDdia2FjNkxRZEhwSlVVeVNIL0VyMjBEWHgzMEt5
aTk3UGNpWEtUUytRS1hubW04aXZ5UkNtdXgyMlpvUFVpbmQyQktDNU9pRzRNd0FMaGFM
MloyazhDc1JkZnkrN2RnN3o0MVJwNkQwWmVFdnRhVXA0Ylg0YUtyYUw0clRmd0lEQVFB
Qm8yQXdYakFNQmdOVkhSTUJBZjhFQWpBQU1BNEdBMVVkRHdFQi93UUVBd0lIZ0RBZEJn
TlZIUTRFRmdRVWt0d2Y2WnBUQ3hqWUt3L0JMVzZQZWlOWDRzd3dId1lEVlIwakJCZ3dG
b0FVdzRNQ25id0Q2bTJ3cG5vUTJzTkQ4R3J5UE40d0RRWUpLb1pJaHZjTkFRRUxCUUFF
Z2dFQkFHdU5IeHYvQlI2ajdsQ1B5c20xdWhyYmpCT3FkcmhKTVIvSWQ0ZEIyR3RkRVNj
bDNpckdQbVh5UTJTbmNUV2hOZnNnc0tEWldwNUJrNytPdG50eTBlTlVNazNoWkVxZ1lq
eGh6YXUwNDhYSGJzZkd2b0phTUdaWk5Ud1V2VFV6Mmhra2hncHg5eVFBS0lBMkx6Rktj
Z1loZWxQdTRHVzVydEV1eHUzSVM2V1l5M0QxR3RGM25hRVdralVyYThoUU9oT2wyUytD
WUhtUmQ2bEdrWHlrVkRhak1nZDJBSkZ6WGRLTHhUdDBPWXJXREdsVVN6R0FDUkJDZDV4
YlJtQVRJbGR0Y2NhR3FETjFjTld2MEkvYlBOOEVwS1M2QjBXYVpjUGFzSXRLV3BEQzg1
SncxR3JEeGRod29LSG94dFNHK29kaVR3QjV6TGJybjJPc1JFNWJWN0U9Il19
.
eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ
```

In Hex:

```
65794A68624763694F694A51557A49314E694973496E67315979493657794A4E5355
6C455A5652445130467452326442643036C435157644A55574A544E454D30516C4E70
5A7A643164556F31645552775A5651305630524254B4A6E6133466F61326C484F58
6377516B465263305A4252454A4954564A4E6430565257557444576B6C7461567051
6555784855554A48556C6C4557544935644531535933644755566C4C5131704A6257
6C6155486C4D5231464352314A5A5346705961476869574541A7A576C524657453143
56556424D565646515864335431567354B4A4A525659305756637864324A485657
6453526B31335347686A546B31555933684E56456C34545652464D55354551586C58
61474E4F5457706A654531715458684E5645313654555242643164715136C4E556B
31335256465A53304E6153573170576C423554456452516B64535755525A4D6A6C30
54564A6A64305A525755744457B6C7461567051655578485554A48556C6C49576C
686F61474A59516E4E615645565A54554A5A523045785655564264336451565778F
516B6C46566A525A567A4633596B64565A314656546C524E53556C4353577042546B
4A6E6133466F61326C484F586377516B465252555A42515539445156453451553314A
53554A445A307444515646465157744F636C424A516B5259545655325A6D4E35646A
56704B314649555546524B3073345A334E444D30684B596A644757685A59586334
```

```
61466869546B70684B3351346354427352457433544670 6E5556685A5669746D5A6C
```

61466869546B70684B335134635442735245743354467 06E5556685A5669746D5A6C

```
61466869546B70684B33513463544273524574335446706E5556685A5669746D5A6C
6434574570324E556448636D7861525452485654557962475A4E5257566E56455236
57565279556C457A644756775A307447616B31485A7A5A4A65545A6D61327778576B
357A65444A6E52573975633235735532686D656B453552307033556C527464457451
596D73786379746F6433677853565531515651725155 6C6C62453578516D646A526A
4A3252545658 4D6A557655306448516D3968556B39575A46565A654846465645526E
5A303078656A566A53315930576D7045576A6772624767306231 5A434D4464696132
466A4E6B78525A456877536C565665564E494C3056794D6A42455748677A4D457435
61546B3355474E705745745555797452533168756257303461585A35556B4E746458
67794D6C70765546567 0626D5179516B74444E553970527A524E6430464D6147464D
4D6C6F79617A684463314A6B5A6E6B724E32526E4E336F304D564A774E6B5177576D
5646646E526856584130596C67305955747959557730636C526D64306C4551564642
516D387951586459616B464E516D644F566B685354554A425A6A6846515770425155
31424E4564424D56566B5248644651693933355555564264306C495A3052425A454A6E
546C5A4955545246526D6452565774306432593257 6E4255513368715755 74334C30
4A4D567A5A515A576C4F5744527A6433644964316C45566C4977616B4A435A336447
62304656647A524E51323569643051326254 4A33634735765554 4A7A546B51345233
4A3555453430643052525755704C6231704A61485A6A546B46525255784355554645
5A326446516B46486455354965485976516C4932616A6473513142356332307864 57
6879596D70435433466B636D684B5456497653575130 5A4549795233526B52564E6A
62444E70636B645162566835555 44A54626D4E555632684F5A6E4E6E63307445576C
64774E554A724E7974506447353065544 26C546C564E617A4E6F576B56785A316C71
654768365958557 74E44685953474A7A5A6B64326230706854556461576B35556431
563256465636 4D6D68726132686E6348673565556464253306C424D6B7836526B746A
5A316C6F5A57785164545248567A5679644556316548557A53564D3256316C354D30
5178523352474D3235685256647 2616C56795954686F5555396F5432777955797444
57556874556D51326245647257486C72566B5268616B316E5A444A42536B5A365747
524C5448685564444250575 84A585245647356564E3652304644556B4A445A445634
596C4A745156524A6247523059324E6852334645546A466A546C64324D456B76596C
424F4F45567753314D32516A42585956706A5547467A5358524C56334245517A6731
536E637852334A456547526F6432394C5347393464464E484B32396B61565233516A
563654474A79626A4A5063314A464E574A574E305539496C31392E65794A4251314D
675258426F5A57316C636D467349464231596D78705979424C5A586B674B4646554B
53493665794A7264 486B694F694A4651794973496D4E79646 94936496C41744D6A55
3249697769654349364 96D3151565574555832 4A42563064495357686E4D46527761
6D7078566E4E514D584A5956314631 58335A33566B39495348524F6132525A623045
694C434A35496A6F694F454A5251584E4A6255646C51564D304E6D5A355633633154
57686D5231 52554D456C71516E4247647A4A54557A4D305248593053584A7A496978
394C434A5452457 3675258426F5A57316C636D467349464231596D78705979424C5A
586B674B4646444B53493665794A7264486B694F694A4651794973496D4E79646949
36496C41744D6A55324969 7769654349364 96C706C4D6D78765531597A64334A7962
307456546C3830656D6833523268446357387A574768314D58526B4E4646715A5645
3164306C57556A41694C434A35496A6F695347784D6447525951564A5A583259314E
55457A5A6D353655574A5159323032614764794D7A524E634468774C573531656C46
44525442616479497366537769 51554E544946654946565354434936496D6830644841364C
79396859334E7A5A584A325A5849755A47397459576C75626D46745A53356A623230
696651
```

```
3A2883E696F07BFD30AC6FE3EB52E653189D0734DB507C995EB284F5E7D1CA512030
9CB46B16092CE52C84896888A31EC4F768C83769655E69310479F3CABEBAE51FB2C2
A90D78F7742AC8954084C20B38C9F201014C1DD8D1E80E0DB4C36E5E93434F1FD455
FD3F3AEC30172230D6C9DD88CB4645BC97874AB46C9323D8EF93C0FE60142296A169
6DB4AF12471CCC86B96C766F22B19C8C7A1B5E2F5C238FA75C44BF8F4AC4A5AB8052
D2DFF1AD558B8D0EA402E6995E1DDE1DACB2926EAD5B8F0A84335A2C60466FC3DCBE
7F5BD0631010F06244B62F45FF7D3D1950994967B5A32343639D66A3E0708B2A23A0
20CFC500CE4E9EA0E25A7AE7AB5440D5B5EA
```

Base64url encoded

```
OiiD5pbwe_0wrG_j61LmUxidBzTbUHyZXrKE9efRylEgMJy0axYJLOUshIloiKMexPdo
yDdpZV5pMQR588q-
uuUfssKpDXj3dCrIlUCEwgs4yfIBAUwd2NHoDg20w25ek0NPH9RV_T867DAXIjDWyd2I
y0ZFvJeHSrRskyPY75PA_mAUIpahaW20rxJHHMyGuWx2byKxnIx6G14vXCOPp1xEv49K
xKWrgFLS3_GtVYuNDqQC5pleHd4drLKSbq1bjwqEM1osYEZvw9y-
f1vQYxAQ8GJEti9F_309GVCZSWe1oyNDY51mo-
BwiyojoCDPxQDOTp6g4lp656tUQNW16g
```

Resulting JWS looks like

JWS Protected Header

Payload

Signature

In Compact Serialization

```
eyJhbGciOiJQUzI1NiIsIng1YyI6WyJNSUlEZVRDQ0FtR2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V0RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSRk13SGhjTk1UY3hNVEl4TVRFMU5EQXlX
aGNOTWpjeE1qTXhNVE16TURBd1dqQklNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVZTUJZR0ExVUVBd3dQVWxO
QklFVjRZVzF3YkdVZ1FVTlRNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1J
SUJDZ0tDQVFFQWtOclBJQkRYTVU2ZmN5djVpK1FIUUFRK0s4Z3NDM0hKYjdGWWhZYXc4
aFhiTkphK3Q4cTBsREt3TFpnUVhZVitmZld4WEp2NUdHcmxaRTRHVTUybGZNRWVnVER6
WVRyUlEzdGVwZ0tGak1HZzZJeTZma2wxWk5zeDJnRW9uc25sU2hmekE5R0p3UlRtdEtQ
Ymsxcytod3gxSVU1QVQrQUllbE5xQmdjRjJ2RTVXMjUvU0dHQm9hUk9WZFVZeHFFVERn
Z00xejVjS1Y0WmpEWjgrbGg0b1ZCMDdia2FjNkxRZEhwSlVVeVNIL0VyMjBEWHgzMEt5
aTk3UGNpWEtUUytRS1hubW04aXZ5UkNtdXgyMlpvUFVpbmQyQktDNU9pRzRNd0FMaGFM
MloyazhDc1JkZnkrN2RnN3o0MVJwNkQwWmVFdnRhVXA0Ylg0YUtyYUw0clRmd0lEQVFB
Qm8yQXdYakFNQmdOVkhSTUJBZjhFQWpBQU1BNEdBMVVkRHdFQi93UUVBd0lIZ0RBZEJn
TlZIUTRFRmdRVWt0d2Y2WnBUQ3hqWUt3L0JMVzZQZWlOWDRzd3dId1lEVlIwakJCZ3dG
b0FVdzRNQ25id0Q2bTJ3cG5vUTJzTkQ4R3J5UE40d0RRWUpLb1pJaHZjTkFRRUxCUUFE
Z2dFQkFHdU5IeHYvQlI2ajdsQ1B5c20xdWhyYmpCT3FkcmhKTVIvSWQ0ZEIyR3RkRVNj
bDNpckdQbVh5UTJTbmNUV2hOZnNnc0tEWldwNUJrNytPdG50eTBlTlVNazNoWkVxZ1lq
eGh6YXUwNDhYSGJzZkd2b0phTUdaWk5Ud1V2VFV6Mmhra2hncHg5eVFBS0lBMkx6Rktj
Z1loZWxQdTRHVzVydEV1eHUzSVM2V1l5M0QxR3RGM25hRVdralVyYThoUU9oT2wyUytD
WUhtUmQ2bEdrWHlrVkRhak1nZDJBSkZ6WGRLTHhUdDBPWXJXREdsVVN6R0FDUkJDZDV4
YlJtQVRJbGR0Y2NhR3FETjFjTld2MEkvYlBOOEVwS1M2QjBXYVpjUGFzSXRLV3BEQzg1
SncxR3JEeGRod29LSG94dFNHK29kaVR3QjV6TGJybjJPc1JFNWJWN0U9Il19

.

eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ

.

OiiD5pbwe_0wrG_j61LmUxidBzTbUHyZXrKE9efRylEgMJy0axYJLOUshIloiKMexPdo
yDdpZV5pMQR588q-
uuUfssKpDXj3dCrIlUCEwgs4yfIBAUwd2NHoDg20w25ek0NPH9RV_T867DAXIjDWyd2I
y0ZFvJeHSrRskyPY75PA_mAUIpahaW20rxJHHMyGuWx2byKxnIx6G14vXCOPp1xEv49K
xKWrgFLS3_GtVYuNDqQC5pleHd4drLKSbq1bjwqEM1osYEZvw9y-
f1vQYxAQ8GJEti9F_309GVCZSWe1oyNDY51mo-
BwiyojoCDPxQDOTp6g4lp656tUQNW16g
```

SDK Validation

The message to validate is (before removing whitespace):

```
eyJhbGciOiJQUzI1NiIsIng1YyI6WyJNSUlEZVRDQ0FtR2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V0RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSk13SGhjTk1UY3hNVEl4TVRFMU5EQXlX
aGNOTWpjeE1qTXhNVE16TURBd1dqQklNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVZTUJZR0ExVUVBd3dQVWxO
QklFVjRZVzF3YkdVZ1FVTlRNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQVE4QU1J
SUJDZ0tDQVFFQWtOclBJQkRYTVU2ZmN5djVpK1FIUUFRK0s4Z3NDM0hKYjdGWWhZYXc4
aFhiTkphK3Q4cTBsREt3TFpnUVhZVitmZld4WEp2NUdHcmxaRTRHVTUybGZNRWVnVER6
WVRyUlEzdGVwZ0tGak1HZzZJeTZma2wxWk5zeDJnRW9uc25sU2hmekE5R0p3UlRtdEtQ
Ymsxcytod3gxSVU1QVQrQUllbE5xQmdjRjJ2RTVXMjUvU0dHQm9hUk9WZFVZeHFFVERn
Z00xejVjS1Y0WmpEWjgrbGg0b1ZCMDdia2FjNkxRZEhwSlVVeVNIL0VyMjBEWHgzMEt5
aTk3UGNpWEtUUytRS1hubW04aXZ5UkNtdXgyMlpvUFVpbmQyQktDNU9pRzRNd0FMaGFM
MloyazhDc1JkZnkrN2RnN3o0MVJwNkQwWmVFdnRhVXA0Ylg0YUtyYUw0clRmd0lEQVFB
Qm8yQXdYakFNQmdOVkhSTUJBZjhFQWpBQU1BNEdBMVVkRHdFQi93UUVBd0lIZ0RBZEJn
TlZIUTRFRmdRVWt0d2Y2WnBUQ3hqWUt3L0JMVzZQZWlOWDRzd3dId1lEVlIwakJCZ3dG
b0FVdzRNQ25id0Q2bTJ3cG5vUTJzTkQ4R3J5UE40d0RRWUpLb1pJaHZjTkFRRUxCUUFE
Z2dFQkFHdU5IeHYvQlI2ajdsQ1B5c20xdWhyYmpCT3FkcmhKTVIvSWQ0ZEIyR3RkRVNj
bDNpckdQbVh5UTJTbmNUV2hOZnNnc0tEWldwNUJrNytPdG50eTBlTlVNazNoWkVxZ1lq
eGh6YXUwNDhYSGJzZkd2b0phTUdaWk5Ud1V2VFV6Mmhra2hncHg5eVFBS0lBMkx6Rktj
Z1loZWxQdTRHVzVydEV1eHUzSVM2V1l5M0QxR3RGM25hRVdralVyYThoUU9oT2wyUytD
WUhtUmQ2bEdrWHlrVkRhak1nZDJBSkZ6WGRLTHhUdDBPWXJXREdsVVN6R0FDUkJDZDV4
YlJtQVRJbGR0Y2NhR3FETjFjTld2MEkvYlBOOEVwS1M2QjBXYVpjUGFzSXRLV3BEQzg1
SncxR3JEeGRod29LSG94dFNHK29kaVR3QjV6TGJybjJPc1JFNWJWN0U9Il19
.
eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ
```

The signature is:

```
OiiD5pbwe_0wrG_j61LmUxidBzTbUHyZXrKE9efRylEgMJy0axYJLOUshIloiKMexPdo
yDdpZV5pMQR588q-
uuUfssKpDXj3dCrIlUCEwgs4yfIBAUwd2NHoDg20w25ek0NPH9RV_T867DAXIjDWyd2I
y0ZFvJeHSrRskyPY75PA_mAUIpahaW20rxJHHMyGuWx2byKxnIx6G14vXCOPp1xEv49K
xKWrgFLS3_GtVYuNDqQC5pleHd4drLKSbq1bjwqEM1osYEZvw9y-
f1vQYxAQ8GJEti9F_309GVCZSWe1oyNDY51mo-
BwiyojoCDPxQDOTp6g4lp656tUQNW16g
```

The SDK unwraps the header thus

```
{"alg":"PS256","x5c":["MIIDeTCCAmGgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WDANB
gkqhkiG9w0BAQsFADBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBG
RYHZXhhbXBsZTEXMBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTE1NDAyW
hcNMjcxMjMxMTMzMDAwWjBIMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyL
GQBGRYHZXhhbXBsZTEYMBYGA1UEAwwPUlNBIEV4YW1wbGUgQUNTMIIBIjANBgkqhkiG9
w0BAQEFAAOCAQ8AMIIBCgKCAQEAkNrPIBDXMU6fcyv5i+QHQAQ+K8gsC3HJb7FYhYaw8
hXbNJa+t8q0lDKwLZgQXYV+ffWxXJv5GGrlZE4GU52lfMEegTDzYTrRQ3tepgKFjMGg6
Iy6fkl1ZNsx2gEonsnlShfzA9GJwRTmtKPbk1s+hwx1IU5AT+AIelNqBgcF2vE5W25/S
GGBoaROVdUYxqETDggM1z5cKV4ZjDZ8+lh4oVB07bkac6LQdHpJUUySH/Er20DXx30Ky
i97PciXKTS+QKXnmm8ivyRCmux22ZoPUind2BKC5OiG4MwALhaL2Z2k8CsRdfy+7dg7z
41Rp6D0ZeEvtaUp4bX4aKraL4rTfwIDAQABo2AwXjAMBgNVHRMBAf8EAjAAMA4GA1UdD
wEB/wQEAwIHgDAdBgNVHQ4EFgQUktwf6ZpTCxjYKw/BLW6PeiNX4swwHwYDVR0jBBgwF
oAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZIhvcNAQELBQADggEBAGuNHxv/BR6j7
lCPysm1uhrbjBOqdrhJMR/Id4dB2GtdEScl3irGPmXyQ2SncTWhNfsgsKDZWp5Bk7+Ot
nty0eNUMk3hZEqgYjxhzau048XHbsfGvoJaMGZZNTwUvTUz2hkkhgpx9yQAKIA2LzFKc
gYhelPu4GW5rtEuxu3IS6WYy3D1GtF3naEWkjUra8hQOhOl2S+CYHmRd6lGkXykVDajM
gd2AJFzXdKLxTt0OYrWDGlUSzGACRBCd5xbRmATIldtccaGqDN1cNWv0I/bPN8EpKS6B
0WaZcPasItKWpDC85Jw1GrDxdhwoKHoxtSG+odiTwB5zLbrn2OsRE5bV7E="]}
```

From this it recovers the public key certificate of the ACS from the x5c parameter and using its copy of the DS public key recovers the ACS key and validates its authenticity.

In this example the DS self signed x.509 root key is as follows:

```
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIQbS4C4BSig7uuJ5uDpeT4VjANBgkqhkiG9w0BAQsFADBH
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHZXhhbXBsZTEX
MBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTE0ODQ5WhcNMjcxMjMx
MTQwMDAwWjBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYH
ZXhhbXBsZTEXMBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCfgQ+0A4Jz0CWR5Ac/MdK2ABuCzttNkvBQFl1Hz8q4
o8Qct3isdVN5P475dXaNGiN02HElZMO813uepDRUSJlAfP8AmZIKkxokxEFIUqsp
vbCpXAZT82xg5gv5C2JY3aVvNwR7pcLR0CmvnJ1AuseqQceKDdEGit1pnoCP6gEe
oUQdik97tOl7459V8d3UTpxLozUVlwPU00tgPmUUek8j1tPAmWx17e6EaoLRkK4Q
eDyWHPA4eu0hBtLQVVtv2Tf61VNTh+D/cv++eJQUArC4IuoqdLYFjB2r+bNKdstj
uH+qLGhHuOKDf/+RGG5rHBSRHPmJqJCSqBzmAd2s0/nPAgMBAAGjRTBDMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBTDgwKdvAPq
bbCmehDaw0PwavI83jANBgkqhkiG9w0BAQsFAAOCAQEAOUcKqpzNQ6lr0PbDSsns
D6onfi+8j3TD0xG0zBSf+8G4zs8Zb6vzzQ5qHKgfr4aeen8Pw0cw2KKUJ2dFaBqj
n3/6/MIZbgaBvXKUbmY8xCxKQ+tOFc3KWIu4pSaO50tMPJjU/lP35bv19AA9vs9M
TKY2qLf88bmoNYT3W8VSDcB58KBHa7HVIPx7BUUtSyb2N2Jqx5AOiYy4NarhB3hV
ftkZBmCzi2Qw50KWIgTFYcIVeRTx3Js/F0IuEdgZHBK2gmO7fdM7+QKYm83401vl
YRNCXfIZ0H9E1V3NddqJuqIutdUajckSzMhXdNCJqfI4FAQAymTWGL3/lZyr/30x
Fg==
-----END CERTIFICATE-----
```

This certificate may be parsed as follows:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6d:2e:02:e0:14:a2:83:bb:ae:27:9b:83:a5:e4:f8:56
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=example, CN=RSA Example DS
        Validity
            Not Before: Nov 21 11:48:49 2017 GMT
            Not After : Dec 31 14:00:00 2027 GMT
        Subject: DC=com, DC=example, CN=RSA Example DS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9f:81:0f:b4:03:82:73:d0:25:91:e4:07:3f:31:
                    d2:b6:00:1b:82:ce:db:4d:92:f0:50:16:5d:47:cf:
                    ca:b8:a3:c4:1c:b7:78:ac:75:53:79:3f:8e:f9:75:
                    76:8d:1a:23:74:d8:71:25:64:c3:bc:d7:7b:9e:a4:
                    34:54:48:99:40:7c:ff:00:99:92:0a:93:1a:24:c4:
                    41:48:52:ab:29:bd:b0:a9:5c:06:53:f3:6c:60:e6:
                    0b:f9:0b:62:58:dd:a5:6f:37:04:7b:a5:c2:d1:d0:
                    29:af:9c:9d:40:ba:c7:aa:41:c7:8a:0d:d1:06:8a:
                    dd:69:9e:80:8f:ea:01:1e:a1:44:1d:8a:4f:7b:b4:
                    e9:7b:e3:9f:55:f1:dd:d4:4e:9c:4b:a3:35:15:97:
                    03:d4:d3:4b:60:3e:65:14:7a:4f:23:d6:d3:c0:99:
                    6c:75:ed:ee:84:6a:82:d1:90:ae:10:78:3c:96:1c:
                    f0:38:7a:ed:21:06:d2:d0:55:5b:6f:d9:37:fa:d5:
                    53:53:87:e0:ff:72:ff:be:78:94:14:02:b0:b8:22:
                    ea:2a:74:b6:05:8c:1d:ab:f9:b3:4a:76:cb:63:b8:
                    7f:aa:2c:68:47:b8:e2:83:7f:ff:91:18:6e:6b:1c:
                    14:91:1c:f9:89:a8:90:92:a8:1c:e6:01:dd:ac:d3:
                    f9:cf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:

C3:83:02:9D:BC:03:EA:6D:B0:A6:7A:10:DA:C3:43:F0:6A:F2:3C:DE
    Signature Algorithm: sha256WithRSAEncryption
         39:47:0a:aa:9c:cd:43:a9:6b:d0:f6:c3:4a:c9:ec:0f:aa:27:
         7e:2f:bc:8f:74:c3:d3:11:b4:cc:14:9f:fb:c1:b8:ce:cf:19:
         6f:ab:f3:cd:0e:6a:1c:a8:1f:af:86:9e:7a:7f:0f:c3:47:30:
         d8:a2:94:27:67:45:68:1a:a3:9f:7f:fa:fc:c2:19:6e:06:81:
         bd:72:94:6e:66:3c:c4:2c:4a:43:eb:4e:15:cd:ca:58:8b:b8:
         a5:26:8e:e7:4b:4c:3c:98:d4:fe:53:f7:e5:bb:f5:f4:00:3d:
         be:cf:4c:4c:a6:36:a8:b7:fc:f1:b9:a8:35:84:f7:5b:c5:52:
         0d:c0:79:f0:a0:47:6b:b1:d5:20:fc:7b:05:45:2d:4b:26:f6:
         37:62:6a:c7:90:0e:89:8c:b8:35:aa:e1:07:78:55:7e:d9:19:
         06:60:b3:8b:64:30:e7:42:96:22:04:c5:61:c2:15:79:14:f1:
         dc:9b:3f:17:42:2e:11:d8:19:1c:12:b6:82:63:bb:7d:d3:3b:
         f9:02:98:9b:cd:f8:d3:5b:e5:61:13:42:5d:f2:19:d0:7f:44:
         d5:5d:cd:75:da:89:ba:a2:2e:b5:d5:1a:8d:c9:12:cc:c8:57:
         74:d0:89:a9:f2:38:14:04:00:ca:64:d6:18:bd:ff:95:9c:ab:
         ff:7d:31:16
```

The key that it recovers is:

Modulus *n* in Hex

```
90DACF2010D7314E9F732BF98BE40740043E2BC82C0B71C96FB1588586B0F215DB34
96BEB7CAB49432B02D98105D857E7DF5B15C9BF9186AE5644E06539DA57CC11E8130
F3613AD1437B5EA602858CC1A0E88CBA7E497564DB31DA01289EC9E54A17F303D189
C114E6B4A3DB935B3E870C75214E404FE0087A536A060705DAF1395B6E7F486181A1
A44E55D518C6A1130E080CD73E5C295E198C367CFA5878A15074EDB91A73A2D0747A
49514C921FF12BDB40D7C77D0ACA2F7B3DC8972934BE40A5E79A6F22BF24429AEC76
D99A0F5229DDD81282E4E886E0CC002E168BD99DA4F02B1175FCBEEDD83BCF8D51A7
A0F465E12FB5A529E1B5F868AADA2F8AD37F
```

Exponent *e* in Hex

```
010001
```

Validation using RSASSA-PSS with SHA-256 of the above message and signature using key modulus “90DA…“with exponent “010001” shows that it is a valid signature.

ACS Signed Content and SDK Validation—EC-based Using ES256

Payload to be signed

```
{
“ACS Ephemeral Public Key (QT)”:{
"kty":"EC",
"crv":"P-256",
"x":"mPUKT_bAWGHIhg0TpjjqVsP1rXWQu_vwVOHHtNkdYoA",
"y":"8BQAsImGeAS46fyWw5MhYfGTT0IjBpFw2SS34Dv4Irs",
},
“SDK Ephemeral Public Key (QC)”:{
"kty":"EC",
"crv":"P-256",
"x":"Ze2loSV3wrroKUN_4zhwGhCqo3Xhu1td4QjeQ5wIVR0",
"y":"HlLtdXARY_f55A3fnzQbPcm6hgr34Mp8p-nuzQCE0Zw",
},
“ACS URL”:”http://acsserver.domainname.com”
}
```

Without whitespace

```
{“ACS Ephemeral Public Key (QT)”:{"kty":"EC","crv":"P-
256","x":"mPUKT_bAWGHIhg0TpjjqVsP1rXWQu_vwVOHHtNkdYoA","y":"8BQAsImG
eAS46fyWw5MhfGTT0IjBpFw2SS34Dv4Irs",},“SDK Ephemeral Public Key
(QC)”:{"kty":"EC","crv":"P-
256","x":"Ze2loSV3wrroKUN_4zhwGhCqo3Xhu1td4QjeQ5wIVR0","y":"HlLtdXAR
Y_f55A3fnzQbPcm6hgr34Mp8p-nuzQCE0Zw",},“ACS
URL”:”http://acsserver.domainname.com”}
```

BASE64url encoded

```
eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ
```

ACS EC Key Pair

```
{
"kty":"EC",
"crv":"P-256",
"x":"36H4sHOgIrtWIObxvXilx3gwlYfYd1TKjdv8idQlhlI",
"y":"KnwGPyr56s6jvi23qMRMzMBpOnMtnmgYNlx5l8aYzt0",
"d":"6-ySVPXPZBVkZ1t951KFgWL_AQrG_wk9BrmV3v3fs5k"
}
```

The ACS possesses a DS generated X.509 certificate for its ECC signature public key:

```
-----BEGIN CERTIFICATE-----
MIICrTCCAZWgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WTANBgkqhkiG9w0BAQsFADBH
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHZXhhbXBsZTEX
MBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTU0MzI3WhcNMjcxMjMx
MTMzMDAwWjBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYH
ZXhhbXBsZTEXMBUGA1UEAwwORUMgRXhhbXBsZSBBQ1MwWTATBgcqhkjOPQIBBggq
hkjOPQMBBwNCAATfofiwc6Aiu1Yg5vG9eKXHeDCVh9h3VMqN2/yJ1CWGUip8Bj8q
+erOo74tt6jETMzAaTpzLZ5oGDZceZfGmM7do2AwXjAMBgNVHRMBAf8EAjAAMA4G
A1UdDwEB/wQEAwIHgDAdBgNVHQ4EFgQU0AWtDHR/vlQrRAz4aKgJBlnFjEswHwYD
VR0jBBgwFoAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZIhvcNAQELBQADggEB
AEqlERewUCeEttAkC0F16Hjjxfv1Wa8naDmaRL99Q0/qqUN8w0qwpAPF7wn2afLf
aGd+5uZEb1TNYwV9Aw9L/s3BcSTERIl6OEWn+x7ctOmHy2vv7mitaUrileGodenm
/faDdy5VgKYj+KsMVM2sNVaekX+T0swACX9B90unZxa6256t2OJ2QV5zu3sYO1N0
j9v7+yF+Fgx014Nrw7/Xt8ILGF58NxbQhkhkfWSfHtaE5moBAbWRuFTFbkBf45SK
e0UMiU5Lac9xI0O7XCD+zNB5mws4NO2AYvyxHq9X+a64IhXclXngPQMrUqMoLWI1
66gRJSvQEWsILIUtx2wsiYs=
-----END CERTIFICATE-----
```

This certificate may be parsed as follows:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6d:2e:02:e0:14:a2:83:bb:ae:27:9b:83:a5:e4:f8:59
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=example, CN=RSA Example DS
        Validity
            Not Before: Nov 21 15:43:27 2017 GMT
            Not After : Dec 31 13:30:00 2027 GMT
        Subject: DC=com, DC=example, CN=EC Example ACS
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:df:a1:f8:b0:73:a0:22:bb:56:20:e6:f1:bd:78:
                    a5:c7:78:30:95:87:d8:77:54:ca:8d:db:fc:89:d4:
                    25:86:52:2a:7c:06:3f:2a:f9:ea:ce:a3:be:2d:b7:
                    a8:c4:4c:cc:c0:69:3a:73:2d:9e:68:18:36:5c:79:
                    97:c6:98:ce:dd
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Subject Key Identifier:

D0:05:AD:0C:74:7F:BE:54:2B:44:0C:F8:68:A8:09:06:59:C5:8C:4B
            X509v3 Authority Key Identifier:

keyid:C3:83:02:9D:BC:03:EA:6D:B0:A6:7A:10:DA:C3:43:F0:6A:F2:3C:DE
```

```
    Signature Algorithm: sha256WithRSAEncryption
         4a:a5:11:17:b0:50:27:84:b6:d0:24:0b:41:75:e8:78:e3:c5:
         fb:f5:59:af:27:68:39:9a:44:bf:7d:43:4f:ea:a9:43:7c:c3:
         4a:b0:a4:03:c5:ef:09:f6:69:f2:df:68:67:7e:e6:e6:44:6f:
         54:cd:63:05:7d:03:0f:4b:fe:cd:c1:71:24:c4:44:89:7a:38:
         45:a7:fb:1e:dc:b4:e9:87:cb:6b:ef:ee:68:ad:69:4a:e2:95:
         e1:a8:75:e9:e6:fd:f6:83:77:2e:55:80:a6:23:f8:ab:0c:54:
         cd:ac:35:56:9e:91:7f:93:d2:cc:00:09:7f:41:f7:4b:a7:67:
         16:ba:db:9e:ad:d8:e2:76:41:5e:73:bb:7b:18:3b:53:74:8f:
         db:fb:fb:21:7e:16:0c:74:d7:83:6b:c3:bf:d7:b7:c2:0b:18:
         5e:7c:37:16:d0:86:48:64:7d:64:9f:1e:d6:84:e6:6a:01:01:
         b5:91:b8:54:c5:6e:40:5f:e3:94:8a:7b:45:0c:89:4e:4b:69:
         cf:71:23:43:bb:5c:20:fe:cc:d0:79:9b:0b:38:34:ed:80:62:
         fc:b1:1e:af:57:f9:ae:b8:22:15:dc:95:79:e0:3d:03:2b:52:
         a3:28:2d:62:35:eb:a8:11:25:2b:d0:11:6b:08:2c:85:2d:c7:
         6c:2c:89:8b
```

It provides a copy for the SDK in the protected header along with the description of the algorithm that the ACS will use to sign the payload thus:

Protected Header

```
{
“alg”:”ES256”,
“x5c”:
[“MIICrTCCAZWgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WTANBgkqhkiG9w0BAQsFADBH
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHZXhhbXBsZTEX
MBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTU0MzI3WhcNMjcxMjMx
MTMzMDAwWjBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYH
ZXhhbXBsZTEXMBUGA1UEAwwORUMgRXhhbXBsZSBBQ1MwWTATBgcqhkjOPQIBBggq
hkjOPQMBBwNCAATfofiwc6Aiu1Yg5vG9eKXHeDCVh9h3VMqN2/yJ1CWGUip8Bj8q
+erOo74tt6jETMzAaTpzLZ5oGDZceZfGmM7do2AwXjAMBgNVHRMBAf8EAjAAMA4G
A1UdDwEB/wQEAwIHgDAdBgNVHQ4EFgQU0AWtDHR/vlQrRAz4aKgJBlnFjEswHwYD
VR0jBBgwFoAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZIhvcNAQELBQADggEB
AEqlERewUCeEttAkC0F16Hjjxfv1Wa8naDmaRL99Q0/qqUN8w0qwpAPF7wn2afLf
aGd+5uZEb1TNYwV9Aw9L/s3BcSTERIl6OEWn+x7ctOmHy2vv7mitaUrileGodenm
/faDdy5VgKYj+KsMVM2sNVaekX+T0swACX9B90unZxa6256t2OJ2QV5zu3sYO1N0
j9v7+yF+Fgx014Nrw7/Xt8ILGF58NxbQhkhkfWSfHtaE5moBAbWRuFTFbkBf45SK
e0UMiU5Lac9xI0O7XCD+zNB5mws4NO2AYvyxHq9X+a64IhXclXngPQMrUqMoLWI1
66gRJSvQEWsILIUtx2wsiYs=”]
}
```

Note: in continued deference to consistency in the RFCs, the cert is base64 not base64url.

Without whitespace

```
{"alg":"ES256","x5c":["MIICrTCCAZWgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WTANB
gkqhkiG9w0BAQsFADBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBG
RYHZXhhbXBsZTEXMBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTU0MzI3W
hcNMjcxMjMxMTMzMDAwWjBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyL
GQBGRYHZXhhbXBsZTEXMBUGA1UEAwwORUMgRXhhbXBsZSBBQ1MwWTATBgcqhkjOPQIBB
ggqhkjOPQMBBwNCAATfofiwc6Aiu1Yg5vG9eKXHeDCVh9h3VMqN2/yJ1CWGUip8Bj8q+
erOo74tt6jETMzAaTpzLZ5oGDZceZfGmM7do2AwXjAMBgNVHRMBAf8EAjAAMA4GA1UdD
wEB/wQEAwIHgDAdBgNVHQ4EFgQU0AWtDHR/vlQrRAz4aKgJBlnFjEswHwYDVR0jBBgwF
oAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZIhvcNAQELBQADggEBAEqlERewUCeEt
tAkC0F16Hjjxfv1Wa8naDmaRL99Q0/qqUN8w0qwpAPF7wn2afLfaGd+5uZEb1TNYwV9A
w9L/s3BcSTERIl6OEWn+x7ctOmHy2vv7mitaUrileGodenm/faDdy5VgKYj+KsMVM2sN
VaekX+T0swACX9B90unZxa6256t2OJ2QV5zu3sYO1N0j9v7+yF+Fgx014Nrw7/Xt8ILG
F58NxbQhkhkfWSfHtaE5moBAbWRuFTFbkBf45SKe0UMiU5Lac9xI0O7XCD+zNB5mws4N
O2AYvyxHq9X+a64IhXclXngPQMrUqMoLWI166gRJSvQEWsILIUtx2wsiYs="]}
```

BASE64url encoded

```
eyJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUlDclRDQ0FaV2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V1RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSRk13SGhjTk1UY3hNVEl4TVRVME16STNX
aGNOTWpjeE1qTXhNVE16TURBd1dqQkhNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVYTUJVR0ExVUVBd3dPUlVN
Z1JYaGhiWEJzWlNCQlExTXdXVEFUQmdjcWhrak9QUUlCQmdncWhrak9QUU1CQndOQ0FB
VGZvZml3YzZBaXUxWWc1dkc5ZUtYSGVEQ1ZoOWgzVk1xTjIveUoxQ1dHVWlwOEJqOHEr
ZXJPbzc0dHQ2akVUTXpBYVRwekxaNW9HRFpjZVpmR21NN2RvMkF3WGpBTUJnTlZIUk1C
QWY4RUFqQUFNQTRHQTFVZER3RUIvd1FFQXdJSGdEQWRCZ05WSFE0RUZnUVUwQVd0REhS
L3ZsUXJSQXo0YUtnSkJsbkZqRXN3SHdZRFZSMGpCQmd3Rm9BVXc0TUNuYndENm0yd3Bu
b1Eyc05EOEdyeVBONHdEUVlKS29aSWh2Y05BUVFMQlFBRGdnRUJBRXFsRVJld1VDZUV0
dEFrQzBGMTZIamp4ZnYxV2E4bmFEbWFSTDk5UTAvcXFVTjh3MHF3cEFQRjd3bjJhZkxm
YUdkKzV1WkViMVROWXdWOUF3OUwvczNCY1NURVJJbDZPRVduK3g3Y3RPbUh5MnZ2N21p
dGFVcmlsZUdvZGVubS9mYURkeTVWZ0tZaitLc01WTTJzTlZhZWtYK1QwWTTJzTlZhZWtYK1Qwc3dBQ1g5Qjkw
```

Message to be signed: Protected header and Payload with a ‘.’ Separator.

(Whitespace omitted).

```
eyJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUlDclRDQ0FaV2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V1RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSRk13SGhjTk1UY3hNVEl4TVRVME16STNX
aGNOTWpjeE1qTXhNVE16TURBd1dqQkhNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVYTUJVR0ExVUVBd3dPUlVN
Z1JYaGhiWEJzWlNCQlExTXdXVEFUQmdjcWhrak9QUUlCQmdncWhrak9QUU1CQndOQ0FB
VGZvZml3YzZBaXUxWWc1dkc5ZUtYSGVEQ1ZoOWgzVk1xTjIveUoxQ1dHVWlwOEJqOHEr
ZXJPbzc0dHQ2akVUTXpBYVRwekxaNW9HRFpjZVpmR21NN2RvMkF3WGpBTUJnTlZIUk1C
QWY4RUFqQUFNQTRHQTFVZER3RUIvd1FFQXdJSGdEQWRCZ05WSFE0RUZnUVUwQVd0REhS
L3ZsUXJSQXo0YUtnSkJsbkZqRXN3SHdZRFZSMGpCQmd3Rm9BVXc0TUNuYndENm0yd3Bu
b1Eyc05EOEdyeVBONHdEUVlKS29aSWh2Y05BUUVMQlFBRGdnRUJBRXFsRVJld1VDZUV0
dEFrQzBGMTZIamp4ZnYxV2E4bmFEbWFSTDk5UTAvcXFVTjh3MHF3cEFQRjd3bjJhZkxm
YUdkKzV1WkViMVROWXdWOUF3OUwvczNCY1NURVJJbDZPRVduK3g3Y3RPbUh5MnZ2N21p
dGFVcmlsZUdvZGVubS9mYURkeTVWZ0tZaitLc01WTTJzTlZhZWtYK1Qwc3dBQ1g5Qjkw
dW5aeGE2MjU2dDJPSjJRVjV6dTNzWU8xTjBqOXY3K3lGK0ZneDAxNE5ydzcvWHQ4SUxH
RjU4TnhiUWhraGtmV1NmSHRhRTVtb0JBYldSdUZURmJrQmY0NVNLZTBVTWlVNUxhYzl4
STBPN1hDRCt6TkI1bXdzNE5PMkFZdnl4SHE5WCthNjRJaFhjbFhuZ1BRTXJVcU1vTFdJ
MTY2Z1JKU3ZRRVdzSUxJVXR4MndzaVlzPSJdfQ
.
eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ
```

In Hex:

```
65794A68624763694F694A46557A49314E694973496E67315979493657794A4E5355
6C44636C52445130466615632644264306C435157644A55574A544E454D30516C4E70
5A7A643164556F31645552775A56513056315242546B4A6E6133466F61326C484F58
6377516B465263305A4252454A4954564A4E6430565257557444576B6C7461567051
6555784855554A48556C6C455754493564453153593364475566C4C5131704A6257
6C6155486C4D5231464352314A5A5346705961476869957454A7A576C524657453143
565564424D565646515864335431567354 6B4A4A52565930575663786432 4A485657
6453526B31335347686A546B31555933684E56456C3454565256 4D45313653544E58
61474E4F5457706A654531715458684E56453136545552426431647 1516B684E556B
31335256465A53304E6153573170576C42355445645 2516B64535755525A4D6A6C30
54564A6A64305A5257557444576B6C7461567051655578485554A48556C6C49576C
686F61474A59516E4E6156455659 54554A56523045785655564264336450556C564E
5A314A5961476869957454A7A576C4E43516C4578545864585645 4655516D646A6357
6872616B395155556C43516D646E63576872616B395155553143516E644F51304642
56475A765A6D6C33597A5A4261585578575763316 46B63355A557459534756455131
5A6F4F57677A566B3178546A497665556F785131644856576C774F454A714F484572
5A584A50627A63306448513 2616B565554587042595652776 56B78614E5739485246
706A5A56706D5232314E4E3252764D6B4633574770425455 4A6E546C5A49556B3143
51575934525546 7151554 64E51545248515446565A4552335255497664314646 5158
644A534764455157524 35A30355753464530525 55A6E555655775156643052456853
4C335A735558 4A5351586F305955746E536B4A73626B5A7152584E335348645A5246
5A534D4770 43516D6433526D394256586330545 54E75596E64454E6D307964334275
6231457963303545 4F4564796556424F4E48644555566C4B53323961535768325930
354255556 4D516C4642524764 6E52554A4252584673525 64A6C643156445A555630
64454672517A42474D545A49616D70345A6E5978563245 34626D4645625746535444
6B3555544176635846556546A68334D484633634546515 26A6433626A4A685A6B786D
5955646B4B7A5631576B5669 4D56524F5758645 74F5546334F557776637A4E435931
4E5552564A4A62445A5052566 4754B33673359335250625568354D6E5A324E323170
64474656636D6C735A5564765A4756756253396D5955526B655456575A30745A6169
744C633031575454 4A7A546C5A685A5774594B315177633364425131673551 6A6B77
64573561654745324D6A5532644 44A50536A4A52566A56366454 4E7A57553878546A
42714F5859334B336C474B305A6E654441784E45357964 7A637657485134535557848
526A5534546E686955576872614 7746D56314E6D534852685254 567462304A42596C
645364555A55526D4A72516D59304E564E4C5A5442565 4576C564E557868597A6C34
535442504E3168445243743654 6B4931625864 7A4E4535504D6B465A646E6C345348
45355743746 84E6A524A614 6686A624668755A31425254584A5663553176 5446644A
4D5459325A314A4B55335A5252566 47A5355784A565852344D6E647A61566C7A5053
4A6466512E65794A4251314D675258426F5A57316C636D4 67349464231596D787059
79424C5A586B674B4646554B5349366579 4A72644 86B694F694A465179 4973496D4E
79646949364 96C41744D6A55324969 77696543493 6496D3151565574555 8324A4256
30644953576 86E4D4652776 16D707856 6E4E514D584A5956314 63158335A33566B39
495348524F6132525A62304 5694C434A35496A6F694F454A5251584E4A6255646C51
564D304E6D5A3556336 3315457686D523152554D456C71516E4247647A4A54557A4D
30524859305358 4A7A49697839 4C434A5452457367 5258426F5A57316C636D467349
464231596D787059794 24C5A586B674B4646444B5349366579 4A7264486B694F694A
465179 4973496D4E796469 4936496C41744D6A55324969 77696543493 6496C706C4D
6D78765531597A64334A79623074 56546C3830656D6833523268446357387A574768
314D58526B4E4646715A56453164306C57556A41694C434A35496A6F695347784D64
47525951564A5A583259314E55457A5A6D353655574A51593230326147 64794D7A52
4E634468774C573531656C4644452544261647949736653776 951554E544946565354
434936496D683064 4841364C79396859334E7A5A584A325A584975 5A47397459576C
75626D46745A53356A623230696651
```

Signature

Signing using EC256 with private key ”6-yS…” produces:

```
28C36DC72DDE64C0E75512BF519BC5B5163C7C3B800072571C268A9DCA15881DDDCB
9EAEE55393D179C1F0AFB49D6C058705A6C14D71195C2298171FC4DA6508
```

Base64url encoded

```
KMNtxy3eZMDnVRK_UZvFtRY8fDuAAHJXHCaKncoViB3dy56u5VOT0XnB8K-
0nWwFhwWmwU1xGVwimBcfxNplCA
```

Resulting JWS looks like

JWS Protected Header

Payload

Signature

In Compact Serialization

```
eyJhbGciOiJFUzI1NiIsIng1YyI6WyJNSUlDclRDQ0FaV2dBd0lCQWdJUWJTNEM0QlNp
Zzd1dUo1dURwZVQ0V1RBTkJna3Foa2lHOXcwQkFRc0ZBREJITVJNd0VRWUtDWkltaVpQ
eUxHUUJHUllEWTI5dE1SY3dGUVlLQ1pJbWlaUHlMR1FCR1JZSFpYaGhiWEJzWlRFWE1C
VUdBMVVFQXd3T1VsTkJJRVY0WVcxd2JHVWdSRk13SGhjTk1UY3hNVEl4TVRVME16STNX
aGNOTWpjeE1qTXhNVE16TURBd1dqQkhNUk13RVFZS0NaSW1pWlB5TEdRQkdSWURZMjl0
TVJjd0ZRWUtDWkltaVpQeUxHUUJHUllIWlhoaGJYQnNaVEVYTUJVR0ExVUVBd3dPUlVN
Z1JYaGhiWEJzWlNCQlExTXdXVEFUQmdjcWhrak9QUUlCQmdncWhrak9QUU1CQndOQ0FB
VGZvZml3YzZBaXUxWWc1dkc5ZUtYSGVEQ1ZoOWgzVk1xTjIveUoxQ1dHVWlwOEJqOHEr
ZXJPbzc0dHQ2akVUTXpBYVRwekxaNW9HRFpjZVpmR21NN2RvMkF3WGpBTUJnTlZIUk1C
QWY4RUFqQUFNQTRHQTFVZER3RUIvd1FFQXdJSGdEQWRCZ05WSFE0RUZnUVVUwQVd0REhS
L3ZsUXJSQXo0YUtnSkJsbkZqRXN3SHdZRFZSMGpCQmd3Rm9BVXc0TUNuYndENm0yd3Bu
b1Eyc05EOEdyeVBONHdEUVlKS29aSWh2Y05BUUVMQlFBRGdnRUJBRXFsRVJld1VDZUV0
dEFrQzBGMTZIamp4ZnYxV2E4bmFEbWFSTDk5UTAvcXFVTjh3MHF3cEFQRjd3bjJhZkxm
YUdkKzV1WkViMVROWXdWOUF3OUwvczNCY1NURVJJbDZPRVduK3g3Y3RPbUh5MnZ2N21p
dGFVcmlsZUdvZGVubS9mYURkeTVWZ0tZaitLc01WTTJzTlZhZWtYK1Qwc3dBQ1g5Qjkw
dW5aeGE2MjU2dDJPSjJRVjV6dTNzWU8xTjBqOXY3K3lGK0ZneDAxNE5ydzcvWHQ4SUxH
RjU4TnhiUWhraGtmV1NmSHRhRTVtb0JBYldSdUZURmJrQmY0NVNLZTBVTWlVNUxhYzl4
STBPN1hDRCt6TkI1bXdzNE5PMkFZdnl4SHE5WCthNjRJaFhjbFhuZ1BRTXJVcU1vTFdJ
MTY2Z1JKU3ZRRVdzSUxJVXR4MndzaVlzPSJdfQ

.

eyJBQ1MgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFUKSI6eyJrdHkiOiJFQyIsImNydiI6
IlAtMjU2IiwieCI6Im1QVUtUX2JBV0dISWhnMFRwampxVnNQMXJYV1F1X3Z3Vk9ISHRO
a2RZb0EiLCJ5IjoiOEJRQXNJbUdlQVM0NmZ5V3c1TWhmR1RUMElqQnBGdzJTUzM0RHY0
SXJzIix9LCJTREsgRXBoZW1lcmFsIFB1YmxpYyBLZXkgKFFDKSI6eyJrdHkiOiJFQyIs
ImNydiI6IlAtMjU2IiwieCI6IlplMmxvU1Yzd3Jyb0tVTl80emh3R2hDcW8zWGh1MXRk
NFFqZVE1d0lWUjAiLCJ5IjoiSGxMdGRYQVJZX2Y1NUEzZm56UWJQY202aGdyMzRNcDhw
LW51elFDRTBadyIsfSwiQUNTIFVSTCI6Imh0dHA6Ly9hY3NzZXJ2ZXIuZG9tYWlubmFt
ZS5jb20ifQ

.

KMNtxy3eZMDnVRK_UZvFtRY8fDuAAHJXHCaKncoViB3dy56u5VOT0XnB8K-
0nWwFhwWmwU1xGVwimBcfxNplCA
```

SDK Validation

The SDK unpacks the protected header thus to determine signature method

```
{"alg":"ES256","x5c":["MIICrTCCAZWgAwIBAgIQbS4C4BSig7uuJ5uDpeT4WTANB
gkqhkiG9w0BAQsFADBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBG
RYHZXhhbXBsZTEXMBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTU0MzI3W
hcNMjcxMjMxMTMzMDAwWjBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyL
GQBGRYHZXhhbXBsZTEXMBUGA1UEAwwORUMgRXhhbXBsZSBBQ1MwWTATBgcqhkjOPQIBB
ggqhkjOPQMBBwNCAATfofiwc6Aiu1Yg5vG9eKXHeDCVh9h3VMqN2/yJ1CWGUip8Bj8q+
erOo74tt6jETMzAaTpzLZ5oGDZceZfGmM7do2AwXjAMBgNVHRMBAf8EAjAAMA4GA1UdD
wEB/wQEAwIHgDAdBgNVHQ4EFgQU0AWtDHR/vlQrRAz4aKgJBlnFjEswHwYDVR0jBBgwF
oAUw4MCnbwD6m2wpnoQ2sND8GryPN4wDQYJKoZIhvcNAQELBQADggEBAEqlERewUCeEt
tAkC0F16Hjjxfv1Wa8naDmaRL99Q0/qqUN8w0qwpAPF7wn2afLfaGd+5uZEb1TNYwV9A
w9L/s3BcSTERIl6OEWn+x7ctOmHy2vv7mitaUrileGodenm/faDdy5VgKYj+KsMVM2sN
VaekX+T0swACX9B90unZxa6256t2OJ2QV5zu3sYO1N0j9v7+yF+Fgx014Nrw7/Xt8ILG
F58NxbQhkhkfWSfHtaE5moBAbWRuFTFbkBf45SKe0UMiU5Lac9xI0O7XCD+zNB5mws4N
O2AYvyxHq9X+a64IhXclXngPQMrUqMoLWI166gRJSvQEWsILIUtx2wsiYs="]}
```

From this it also recovers the public key certificate of the ACS from the x5c parameter and using its copy of the DS public key recovers the ACS key and validates its authenticity.

In this example the DS self signed x.509 root key is as follows:

```
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIQbS4C4BSig7uuJ5uDpeT4VjANBgkqhkiG9w0BAQsFADBH
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHZXhhbXBsZTEX
MBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwHhcNMTcxMTIxMTE0ODQ5WhcNMjcxMjMx
MTQwMDAwWjBHMRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYH
ZXhhbXBsZTEXMBUGA1UEAwwOUlNBIEV4YW1wbGUgRFMwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQCfgQ+0A4Jz0CWR5Ac/MdK2ABuCzttNkvBQFl1Hz8q4
o8Qct3isdVN5P475dXaNGiN02HElZMO813uepDRUSJlAfP8AmZIKkxokxEFIUqsp
vbCpXAZT82xg5gv5C2JY3aVvNwR7pcLR0CmvnJ1AuseqQceKDdEGit1pnoCP6gEe
oUQdik97tOl7459V8d3UTpxLozUVlwPU00tgPmUUek8j1tPAmWx17e6EaoLRkK4Q
eDyWHPA4eu0hBtLQVVtv2Tf61VNTh+D/cv++eJQUArC4IuoqdLYFjB2r+bNKdstj
uH+qLGhHuOKDf/+RGG5rHBSRHPmJqJCSqBzmAd2s0/nPAgMBAAGjRTBDMBIGA1Ud
EwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBTDgwKdvAPq
bbCmehDaw0PwavI83jANBgkqhkiG9w0BAQsFAAOCAQEAOUcKqpzNQ6lr0PbDSsns
D6onfi+8j3TD0xG0zBSf+8G4zs8Zb6vzzQ5qHKgfr4aeen8Pw0cw2KKUJ2dFaBqj
n3/6/MIZbgaBvXKUbmY8xCxKQ+tOFc3KWIu4pSaO50tMPJjU/lP35bv19AA9vs9M
TKY2qLf88bmoNYT3W8VSDcB58KBHa7HVIPx7BUUtSyb2N2Jqx5AOiYy4NarhB3hV
ftkZBmCzi2Qw50KWIgTFYcIVeRTx3Js/F0IuEdgZHBK2gmO7fdM7+QKYm83401vl
YRNCXfIZ0H9E1V3NddqJuqIutdUajckSzMhXdNCJqfI4FAQAymTWGL3/lZyr/30x
Fg==
-----END CERTIFICATE-----
```

This certificate may be parsed as:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            6d:2e:02:e0:14:a2:83:bb:ae:27:9b:83:a5:e4:f8:56
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC=com, DC=example, CN=RSA Example DS
        Validity
            Not Before: Nov 21 11:48:49 2017 GMT
            Not After : Dec 31 14:00:00 2027 GMT
        Subject: DC=com, DC=example, CN=RSA Example DS
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9f:81:0f:b4:03:82:73:d0:25:91:e4:07:3f:31:
                    d2:b6:00:1b:82:ce:db:4d:92:f0:50:16:5d:47:cf:
                    ca:b8:a3:c4:1c:b7:78:ac:75:53:79:3f:8e:f9:75:
                    76:8d:1a:23:74:d8:71:25:64:c3:bc:d7:7b:9e:a4:
                    34:54:48:99:40:7c:ff:00:99:92:0a:93:1a:24:c4:
                    41:48:52:ab:29:bd:b0:a9:5c:06:53:f3:6c:60:e6:
                    0b:f9:0b:62:58:dd:a5:6f:37:04:7b:a5:c2:d1:d0:
                    29:af:9c:9d:40:ba:c7:aa:41:c7:8a:0d:d1:06:8a:
                    dd:69:9e:80:8f:ea:01:1e:a1:44:1d:8a:4f:7b:b4:
                    e9:7b:e3:9f:55:f1:dd:d4:4e:9c:4b:a3:35:15:97:
                    03:d4:d3:4b:60:3e:65:14:7a:4f:23:d6:d3:c0:99:
                    6c:75:ed:ee:84:6a:82:d1:90:ae:10:78:3c:96:1c:
                    f0:38:7a:ed:21:06:d2:d0:55:5b:6f:d9:37:fa:d5:
                    53:53:87:e0:ff:72:ff:be:78:94:14:02:b0:b8:22:
                    ea:2a:74:b6:05:8c:1d:ab:f9:b3:4a:76:cb:63:b8:
                    7f:aa:2c:68:47:b8:e2:83:7f:ff:91:18:6e:6b:1c:
                    14:91:1c:f9:89:a8:90:92:a8:1c:e6:01:dd:ac:d3:
                    f9:cf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:

C3:83:02:9D:BC:03:EA:6D:B0:A6:7A:10:DA:C3:43:F0:6A:F2:3C:DE
    Signature Algorithm: sha256WithRSAEncryption
         39:47:0a:aa:9c:cd:43:a9:6b:d0:f6:c3:4a:c9:ec:0f:aa:27:
         7e:2f:bc:8f:74:c3:d3:11:b4:cc:14:9f:fb:c1:b8:ce:cf:19:
         6f:ab:f3:cd:0e:6a:1c:a8:1f:af:86:9e:7a:7f:0f:c3:47:30:
         d8:a2:94:27:67:45:68:1a:a3:9f:7f:fa:fc:c2:19:6e:06:81:
         bd:72:94:6e:66:3c:c4:2c:4a:43:eb:4e:15:cd:ca:58:8b:b8:
         a5:26:8e:e7:4b:4c:3c:98:d4:fe:53:f7:e5:bb:f5:f4:00:3d:
         be:cf:4c:4c:a6:36:a8:b7:fc:f1:b9:a8:35:84:f7:5b:c5:52:
         0d:c0:79:f0:a0:47:6b:b1:d5:20:fc:7b:05:45:2d:4b:26:f6:
         37:62:6a:c7:90:0e:89:8c:b8:35:aa:e1:07:78:55:7e:d9:19:
         06:60:b3:8b:64:30:e7:42:96:22:04:c5:61:c2:15:79:14:f1:
```

```
                    dc:9b:3f:17:42:2e:11:d8:19:1c:12:b6:82:63:bb:7d:d3:3b:
                    f9:02:98:9b:cd:f8:d3:5b:e5:61:13:42:5d:f2:19:d0:7f:44:
                    d5:5d:cd:75:da:89:ba:a2:2e:b5:d5:1a:8d:c9:12:cc:c8:57:
                    74:d0:89:a9:f2:38:14:04:00:ca:64:d6:18:bd:ff:95:9c:ab:
                    ff:7d:31:16
```

The key that it recovers is:

```
04DFA1F8B073A022BB5620E6F1BD78A5C778309587D87754CA8DDBFC89D42586522A
7C063F2AF9EACEA3BE2DB7A8C44CCCC0693A732D9E6818365C7997C698CEDD
```

With an OID of “prime256v1”.

Using this key it validates the signature.

ACS Diffie-Hellman and Session Key Derivation—EC-based Using ECDH-ES

This process is used by the ACS to derive a common secret key. The exchange of the ephemeral keys precedes this.

This is ECDH Direct Key Agreement mode ("alg" value "ECDH-ES") with a presumed enc algorithm of "ECDH-ES+A256KW" that is not included as an AlgorithmID in the KDF function in order to output 256 bits of key material. Both EC keys are ephemeral.

SDK Ephemeral Public Key (Q_C)

The SDK generated this ephemeral key and sent it to the ACS

```
{
"kty":"EC",
"crv":"P-256",
"x":"weNJy2HscCSM6AEDTDg04biOvhFhyyWvOHQfeF_PxMQ",
"y":"e8lnCO-AlStT-NJVX-crhB7QRYhiix03illJOVAOyck"
}
```

ACS Ephemeral Key Pair (Q_T, d_T)

The ACS generated this ephemeral keypair and uses it with the SDK ephemeral key:

```
{
"kty":"EC",
"crv":"P-256",
"x":"gI0GAILBdu7T53akrFmMyGcsF3n5dO7MmwNBHKW5SV0",
"y":"SLW_xSffzlPWrHEVI30DHM_4egVwt3NQqeUD7nMFpps",
"d":"0_NxaRPUMQoAJt50Gz8YiTr8gRTwyEaCumd-MToTmIo"
}
```

Perform ECDH operation with Q_C and d_T

The public key point Q_C is as follows in SEC1 format:

```
04C1E349CB61EC70248CE801034C3834E1B88EBE1161CB25AF38741F785FCFC4C47B
C96708EF80952B53F8D2555FE72B841ED04588628B1D378A594939500EC9C9
```

The ACS private key d_T is:

```
D3F3716913D4310A0026DE741B3F18893AFC8114F0C84682BA677E313A13988A
```

The resulting point is d_T• Qc in SEC1 point representation =

```
049E56D91D817135D372834283BF84269CFB316EA3DA806A48F6DAA7798CFE90C4CC
3564FF1BB5F4FA8FFD89EC60791510330D992063CD8B717B96B3E1B6F88098
```

Z = x coordinate:

```
9E56D91D817135D372834283BF84269CFB316EA3DA806A48F6DAA7798CFE90C4
```

Keydatalen = 256 (0x0100).

There is no apu, and apv is the SDK Reference Number.There is no AlgorithmID.

Note: RFC 7518 as referenced in the specification has the ECDH-ES key agreement in section 4.6. This has a sequence that the key agreement feeds directly into either an encryption function or a key wrapping function. Some libraries may be "atomic" in this respect, whereas 3DS requires the CEK to be extracted for later independent use by the CReq/CRes encryption/decryption secure channel. Therefore to obtain 256 bits of keying material (the CEK) from some libraries, it may be necessary to specify an encryption algorithm that will not actually be used and to extract the CEK at an intermediate stage. This is the purpose of the wording in the spec "…assume an "enc" parameter of ECDH-ES+A256KW and assume the algorithmID to be null for the KDF…"

Concat KDF is then used to form the key value as follows:

AlgorithmID = length of 0 + null string as the AlgorithmID is not used in this case = `00000000`

PartyUInfo = length of 0 + null string as there is no apu data: `00000000`

PartyVInfo = length of 28 + "A Dummy SDK Reference Number" = `0000001C 412044756D6D792053444B205265666572656E6365204E756D626572`

SuppPubInfo = Keydatalen = `00000100`

SuppPrivInfo = empty string

Concatenating 1 + Z + AlgorithmID + PartyUInfo + PartyVInfo + SuppPubInfo + SuppPrivInfo =

```
00000001
9E56D91D817135D372834283BF84269CFB316EA3DA806A48F6DAA7798CFE90C4
00000000 00000000 0000001C
412044756D6D792053444B205265666572656E6365204E756D626572 00000100
```

Hashing with SHA-256 yields:

```
4B57071C56A1393B613B05948621D2FAC5D37C30CBEF51D4642A8D1BB22A1C23
```

This is the shared secret key data

For subsequent use, when using A128CBC-HS256, the same key is used in both directions. When using A128GCM, the leftmost 128 bits are $CEK_{S\text{-}A}$ and the rightmost 128 bits $CEK_{A\text{-}S}$.

SDK Diffie-Hellman and Session Key Derivation—EC-based Using ECDH-ES

This is ECDH Direct Key Agreement mode ("alg" value "ECDH-ES") with a presumed enc algorithm of "ECDH-ES+A256KW" that is not included as an AlgorithmID in the KDF function in order to output 256 bits of key material. Both EC keys are ephemeral.

This is the same calculation as the ACS performs to derive the same shared secret key material.

SDK Ephemeral Public Key (Q_C)

The SDK previously generated this ephemeral key

```
{"kty":"EC",
"crv":"P-256",
"x":"weNJy2HscCSM6AEDTDg04biOvhFhyyWvOHQfeF_PxMQ",
"y":"e8lnCO-AlStT-NJVX-crhB7QRYhiix03illJOVAOyck",
"d":"VEmDZpDXXK8p8N0Cndsxs924q6nS1RXFASRl6BfUqdw"
}
```

The ACS previously generated and sent this ephemeral key to the SDK

```
{
"kty":"EC",
"crv":"P-256",
"x":"gI0GAILBdu7T53akrFmMyGcsF3n5dO7MmwNBHKW5SV0",
"y":"SLW_xSffzlPWrHEVI30DHM_4egVwt3NQqeUD7nMFpps",
}
```

Perform ECDH operation with Q_T

received from the ACS (in the signature) and d_C

The public key point from Q_T in SEC1 point representation is:

```
04808D060082C176EED3E776A4AC598CC8672C1779F974EECC9B03411CA5B9495D48
B5BFC527DFCE53D6AC7115237D031CCFF87A0570B77350A9E503EE7305A69B
```

The SDK private key d_C is:

```
5449836690D75CAF29F0DD029DDB31B3DDB8ABA9D2D515C5012465E817D4A9DC
```

The resultant point is $d_C \bullet Q_T$ in SEC1 point representation =

```
049E56D91D817135D372834283BF84269CFB316EA3DA806A48F6DAA7798CFE90C4CC
3564FF1BB5F4FA8FFD89EC60791510330D992063CD8B717B96B3E1B6F88098
```

Z = x coordinate:

```
9E56D91D817135D372834283BF84269CFB316EA3DA806A48F6DAA7798CFE90C4
```

Keydatalen = 256.

There is no apu, and apv is the SDK Reference Number. There is no AlgorithmID.

Note: RFC 7518 as referenced in the specification has the ECDH-ES key agreement in section 4.6. This has a sequence that the key agreement feeds directly into either an encryption function or a key wrapping function. Some libraries may be “atomic” in this respect, whereas 3DS requires the CEK to be extracted for later independent use by the CReq/CRes encryption/decryption secure channel. Therefore to obtain 256 bits of keying material (the CEK) from some libraries, it may be necessary to specify an encryption algorithm that will not actually be used and to extract the CEK at an intermediate stage. This is the purpose of the wording in the spec “…assume an “enc” parameter of ECDH-ES+A256KW and assume the algorithmID to be null for the KDF…”

Concat KDF is then used to form the key value as follows:

AlgorithmID = length of 0 + null string = `00000000`

PartyUInfo = length of 0 + null string as there is no apu data: `00000000`

PartyVInfo = length of 28 + “A Dummy SDK Reference Number” = `0000001C 412044756D6D792053444B205265666572656E6365204E756D626572`

SuppPubInfo = Keydatalen = `00000100`

SuppPrivInfo = empty string

Concatenating 1 + Z + AlgorithmID + PartyUInfo + PartyVInfo + SuppPubInfo + SuppPrivInfo =

```
00000001
9E56D91D817135D372834283BF84269CFB316EA3DA806A48F6DAA7798CFE90C4
00000000 00000000 0000001C
412044756D6D792053444B205265666572656E6365204E756D626572 00000100
```

Hashing with SHA-256 yields:

```
4B57071C56A1393B613B05948621D2FAC5D37C30CBEF51D4642A8D1BB22A1C23
```

This is the shared secret key data, which matches the keys derived by the ACS in the previous example.

For subsequent use, when using A128CBC-HS256, the same key is used in both directions. When using A128GCM, the leftmost 128 bits are CEK_{S-A} and the rightmost 128 bits CEK_{A-S}.

SDK Encryption of CReq and ACS Decryption—Using A128CBC-HS256

CReq Message Contents

Plaintext Data

```
{
      "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
      "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
      "messageType":"CReq",
      "messageVersion":"2.1.0",
      "sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
      "sdkCounterStoA":"001"
}
```

Without whitespace

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","messageType":"CReq","messageVersion":"2.1.0","sdkTran
sID":"b2385523-a66c-4907-ac3c-91848e8c0067","sdkCounterStoA":"001"}
```

CEK from previous DH exchange:

```
4B57071C56A1393B613B05948621D2FAC5D37C30CBEF51D4642A8D1BB22A1C23
```

The first half is the authentication key

```
4B57071C56A1393B613B05948621D2FA
```

The second half is the encryption key

```
C5D37C30CBEF51D4642A8D1BB22A1C23
```

Initialization Vector

For CBC mode a fresh IV is used. In this example:

```
31DB8427DCF25BEEA6C85D0E3F665FEA
```

In base64url

```
MduEJ9zyW-6myF0OP2Zf6g
```

Protected Header

```
{
      "alg":”dir",
      “kid”:”ACSTransactionID”,
      "enc":”A128CBC-HS256"
}
```

Without whitespace

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128CBC-HS256"}
```

base64url encoded

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOENC
Qy1IUzI1NiJ9
```

Data Encipherment

CBC encipherment of the plaintext using AES-128 with key “C5D3 …”; IV “MduE….” with PKCS7 padding produces:

```
124D5AE217D806351169552BA7504326A6CA5481AE04A3E71343AB6FB2EDB7DC991E
B2C8E1783067DD3547D67BD1C57993E280D7E23610901B69599A9956084A025D3EFD
EC69C0416F4230CBBC606ADEEC464D125FC753FBBA5D969A4D81F989B73821CD2C91
A035588804842C5AA9E7CB71C80541B18BA94BBF9DC16E31849C7AAFA822A276F1C2
14D016427EA62D4BD0A44CA7AA4A27DD5749E97D489FA770CD0E292B25EA9B944735
35E5EDA0E0F97E160E71CB3CA61B20C87130DD1EB89F5892E1DE4683C7B8371B1F11
DE3FB9713B4AD08F7928A0A0F2F72829B0AB943A0103321F4456D5DF1BA09C35A75C
6E3B
```

Base64url encoded:

```
Ek1a4hfYBjURaVUrp1BDJqbKVIGuBKPnE0Orb7Ltt9yZHrLI4XgwZ901R9Z70cV5k-
KA1-I2EJAbaVmamVYISgJdPv3sacBBb0Iwy7xgat7sRk0SX8dT-
7pdlppNgfmJtzghzSyRoDVYiASELFqp58txyAVBsYupS7-
dwW4xhJx6r6gionbxwhTQFkJ-pi1L0KRMp6pKJ91XSel9SJ-
ncM0OKSsl6puURzU15e2g4Pl-Fg5xyzymGyDIcTDdHrifWJLh3kaDx7g3Gx8R3j-
5cTtK0I95KKCg8vcoKbCrlDoBAzIfRFbV3xugnDWnXG47
```

Authentication Tag

For the MAC, the Additional Authenticated Data (AAD) is the Protected Header, which as Hex representation of base64url string is

```
“65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636
D46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E4
351793149557A49314E694A39” so the AAD Length (AL) is
0000000000000280 (80 bytes = 640 bits).
```

The data to MAC is the concatenation of AAD (in ASCII), IV, Ciphertext and AL hence the data to MAC in hexadecimal is:

```
65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636D
46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E43
51793149557A49314E694A39
31DB8427DCF25BEEA6C85D0E3F665FEA
124D5AE217D806351169552BA7504326A6CA5481AE04A3E71343AB6FB2EDB7DC991E
B2C8E1783067DD3547D67BD1C57993E280D7E23610901B69599A9956084A025D3EFD
EC69C0416F4230CBBC606ADEEC464D125FC753FBBA5D969A4D81F989B73821CD2C91
A035588804842C5AA9E7CB71C80541B18BA94BBF9DC16E31849C7AAFA822A276F1C2
14D016427EA62D4BD0A44CA7AA4A27DD5749E97D489FA770CD0E292B25EA9B944735
35E5EDA0E0F97E160E71CB3CA61B20C87130DD1EB89F5892E1DE4683C7B8371B1F11
DE3FB9713B4AD08F7928A0A0F2F72829B0AB943A0103321F4456D5DF1BA09C35A75C
6E3B
0000000000000280
```

MACing using HMAC SHA256 and a key of "4B57…" produces:

```
F90F38BC76A6A4C241BAF05AFA78A52AAADD844B0FB927AC3CA4242D56DAD617
```

The most significant 16 bytes are the authentication tag which is

```
F90F38BC76A6A4C241BAF05AFA78A52A
```

Base64url encoded

```
-Q84vHampMJBuvBa-nilKg
```

Resulting JWE looks like

JWE Protected Header

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOENC
Qy1IUzI1NiJ9

.

.

MduEJ9zyW-6myF0OP2Zf6g

.

Ek1a4hfYBjURaVUrp1BDJqbKVIGuBKPnE0Orb7Ltt9yZHrLI4XgwZ901R9Z70cV5k-
KA1-I2EJAbaVmamVYISgJdPv3sacBBb0Iwy7xgat7sRk0SX8dT-
7pdlppNgfmJtzghzSyRoDVYiASELFqp58txyAVBsYupS7-
dwW4xhJx6r6gionbxwhTQFkJ-pi1L0KRMp6pKJ91XSel9SJ-
ncM0OKSsl6puURzU15e2g4Pl-Fg5xyzymGyDIcTDdHrifWJLh3kaDx7g3Gx8R3j-
5cTtK0I95KKCg8vcoKbCrlDoBAzIfRFbV3xugnDWnXG47

.

-Q84vHampMJBuvBa-nilKg
```

ACS Decryption

The ACS unwraps the protected header to yield this

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128CBC-HS256"}
```

From which it understands that it must use AES 128 bit CBC with HMAC-256.

It determines the binary version of the protected header as

```
65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636D
46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E43
51793149557A49314E694A39
```

From which it determines the bitlength as 640 bits and AL as `0000000000000280`

The data to HMAC with key "4B57…." is therefore:

```
65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636D
46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E43
51793149557A49314E694A39
31DB8427DCF25BEEA6C85D0E3F665FEA
124D5AE217D806351169552BA7504326A6CA5481AE04A3E71343AB6FB2EDB7DC991E
B2C8E1783067DD3547D67BD1C57993E280D7E23610901B69599A9956084A025D3EFD
EC69C0416F4230CBBC606ADEEC464D125FC753FBBA5D969A4D81F989B73821CD2C91
A035588804842C5AA9E7CB71C80541B18BA94BBF9DC16E31849C7AAFA822A276F1C2
14D016427EA62D4BD0A44CA7AA4A27DD5749E97D489FA770CD0E292B25EA9B944735
35E5EDA0E0F97E160E71CB3CA61B20C87130DD1EB89F5892E1DE4683C7B8371B1F11
DE3FB9713B4AD08F7928A0A0F2F72829B0AB943A0103321F4456D5DF1BA09C35A75C
6E3B
0000000000000280
```

Giving the hash result (1st 16 bytes)

```
F90F38BC76A6A4C241BAF05AFA78A52A
```

Base64url encoded

```
-Q84vHampMJBuvBa-nilKg
```

Which matches the token in the message

CBC decipherment of message "Ek1a…"using AES-128 with key "C5D3 …"; IV "MduE…." produces:

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","messageType":"CReq","messageVersion":"2.1.0","sdkTran
sID":"b2385523-a66c-4907-ac3c-91848e8c0067","sdkCounterStoA":"001"}
```

Inserting whitespace for clarity:

```
{
      "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
      "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
      "messageType":"CReq",
      "messageVersion":"2.1.0",
      "sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
      "sdkCounterStoA":"001"
}
```

SDK Encryption of CReq and ACS Decryption—Using A128GCM

CReq Message Contents

Plaintext Data

```
{
     "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
     "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
     "messageType":"CReq",
     "messageVersion":"2.1.0",
     "sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
     "sdkCounterStoA":"001"
}
```

Without whitespace

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340","messageType":"CReq","messageVersion":"2.1.0","sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067","sdkCounterStoA":"001"}
```

CEK from previous DH exchange is the leftmost half of the derived key:

```
4B57071C56A1393B613B05948621D2FA
```

Initialization Vector

For GCM mode the IV is the counter left padded with 00 bytes.

The counter is a 1 byte counter and in this example is "001", so the IV would be

```
000000000000000000000001
```

which in base64url format is

```
AAAAAAAAAAAAAAAB
```

Protected Header

```
{
     "alg":”dir",
     “kid”:”ACSTransactionID”,
     "enc":”A128GCM"
}
```

Without whitespace

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128GCM"}
```

BASE64url encoded

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOEdDTSJ9
```

Data Encipherment

GCM encipherment of the plaintext using AES-128 with key “4B57…”; IV “AAAA….”; Protected Header “eyJh…”produces:

```
9CE62D193AD45F852E7907884B9240BC0D878A719CA6BA85CCE8E381E2B7CE056783
1E8AF7D057267808A1CC44971E51D47842A817ED57818C8E9D3CE07726082E1549C7
84292F64A37FFB5BBEADADB4EEC1C4AC4FE0862F7D01422352BC0F2C92DDDEE7B6E3
8F1EFF858776910EA373638323AA5DAF348211B4FDCE738B5E611C9560AA69E8EF5B
2DB3E190F2A677343B7BCBCF85703AD45C924D744285C0A8031F0F70D20CB91DD1A0
F4C67E81DC6E38B7C55B470961BCA69F859B77B2FA835E1CF54855363CA34F9A62B3
2C34A1B66FFB897FB63BBBD96FC8D0246379BB2068F3540F991EFEE9D7EEC46F
```

Base64url encoded:

```
nOYtGTrUX4UueQeIS5JAvA2HinGcprqFzOjjgeK3zgVngx6K99BXJngIocxElx5R1HhC
qBftV4GMjp084HcmCC4VSceEKS9ko3_7W76trbTuwcSsT-
CGL30BQiNSvA8skt3e57bjjx7_hYd2kQ6jc2ODI6pdrzSCEbT9znOLXmEclWCqaejvWy
2z4ZDypnc0O3vLz4VwOtRckk10QoXAqAMfD3DSDLkd0aD0xn6B3G44t8VbRwlhvKafhZ
t3svqDXhz1SFU2PKNPmmKzLDShtm_7iX-2O7vZb8jQJGN5uyBo81QPmR7-6dfuxG8
```

Authentication Tag

```
316819A346E6235F54DCC905427E4CCA
```

In base64url:

```
MWgZo0bmI19U3MkFQn5Myg
```

Resulting JWE looks like

JWE Protected Header

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOEdD
TSJ9

.

.

AAAAAAAAAAAAAAAB

.

nOYtGTrUX4UueQeIS5JAvA2HinGcprqFzOjjgeK3zgVngx6K99BXJngIocxElx5R1HhC
qBftV4GMjp084HcmCC4VSceEKS9ko3_7W76trbTuwcSsT-
CGL30BQiNSvA8skt3e57bjjx7_hYd2kQ6jc2ODI6pdrzSCEbT9znOLXmEclWCqaejvWy
2z4ZDypnc0O3vLz4VwOtRckk10QoXAqAMfD3DSDLkd0aD0xn6B3G44t8VbRwlhvKafhZ
t3svqDXhz1SFU2PKNPmmKzLDShtm_7iX-2O7vZb8jQJGN5uyBo81QPmR7-6dfuxG8

.

MWgZo0bmI19U3MkFQn5Myg
```

ACS Decryption

The ACS unwraps the protected header to yield this

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128GCM"}
```

From which it understands that it must use AES 128 bit GCM.

GCM decipherment of the message “nOYt…” using Additional Authenticated Data “eyJh…”; IV “AAAA…”; Authentication Tag “MWgZ…”; key ”4B57…“ produces:

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","messageType":"CReq","messageVersion":"2.1.0","sdkTran
sID":"b2385523-a66c-4907-ac3c-91848e8c0067","sdkCounterStoA":"001"}
```

Inserting whitespace for clarity:

```
{
     "threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
     "acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
     "messageType":"CReq",
     "messageVersion":"2.1.0",
     "sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
     "sdkCounterStoA":"001"
     }
```

ACS Encryption of CRes and SDK Decryption—Using A128CBC-HS256

CReq Message Contents

Plaintext Data

```
{
"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
"acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
"uiType":"01",
"challengeAddInfo":"Additional information to be shown.",
"challengeCompletionInd":"N",
"challengeInfoHeader":"Header information",
"challengeInfoLabel":"One-time-password",
"challengeInfoText":"Please enter the received one-time-password",
"challengeInfoTextIndicator":"N",
"expandInfoLabel1":"Additional instructions",
"expandInfoText1":"The issuer will send you via SMS a one-time
password. Please enter the value in the designated input field above
and press continue to complete the 3-D Secure authentication
process.",
"issuerImage":{
      "medium":"http://acs.com/medium_image.svg",
      "high":"http://acs.com/high_image.svg",
      "extraHigh":"http://acs.com/extraHigh_image.svg"
},
"messageType":"CRes",
"messageVersion":"2.1.0",
"psImage": {
      "medium":"http://ds.com/medium_image.svg",
      "high":"http://ds.com/high_image.svg",
      "extraHigh":"http://ds.com/extraHigh_image.svg"
},
"resendInformationLabel":"Send new One-time-password",
"sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
"submitAuthenticationLabel":"Continue",
"whyInfoLabel1":"Why using 3-D Secure?",
"whyInfoText1":"Some explanation about why using 3-D Secure is an
excellent idea as part of an online payment transaction",
"acsCounterAtoS":"001"
}
```

Without whitespace

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","uiType":"01","challengeAddInfo":"Additional
information to be shown.",
"challengeCompletionInd":"N","challengeInfoHeader":"Header
information","challengeInfoLabel":"One-time-
password","challengeInfoText":"Please enter the received one-time-
password","challengeInfoTextIndicator":"N","expandInfoLabel1":"Addit
ional instructions","expandInfoText1":"The issuer will send you via
SMS a one-time password. Please enter the value in the designated
input field above and press continue to complete the 3-D Secure
authentication
process.","issuerImage":{"medium":"http://acs.com/medium_image.svg",
"high":"http://acs.com/high_image.svg","extraHigh":"http://acs.com/e
xtraHigh_image.svg"},"messageType":"CRes","messageVersion":"2.1.0","
psImage":
{"medium":"http://ds.com/medium_image.svg","high":"http://ds.com/hig
h_image.svg","extraHigh":"http://ds.com/extraHigh_image.svg"},"resen
dInformationLabel":"Send new One-time-
password","sdkTransID":"b2385523-a66c-4907-ac3c-
91848e8c0067","submitAuthenticationLabel":"Continue","whyInfoLabel1"
:"Why using 3-D Secure?","whyInfoText1":"Some explanation about why
using 3-D Secure is an excellent idea as part of an online payment
transaction","acsCounterAtoS":"001"}
```

CEK from previous DH exchange:

```
4B57071C56A1393B613B05948621D2FAC5D37C30CBEF51D4642A8D1BB22A1C23
```

The first half is the authentication key

```
4B57071C56A1393B613B05948621D2FA
```

The second half is the encryption key

```
C5D37C30CBEF51D4642A8D1BB22A1C23
```

Initialization Vector

For CBC mode a fresh IV is used. In this example:

```
BE94AECB5F6706EE3BC88EAE1E5938A9
```

In base64url

```
vpSuy19nBu47yI6uHlk4qQ
```

Protected Header

```
{
     "alg":”dir",
     “kid”:”ACSTransactionID”,
     "enc":”A128CBC-HS256"
}
```

Without whitespace

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128CBC-HS256"}
```

BASE64url encoded

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOENC
Qy1IUzI1NiJ9
```

Data Encipherment

CBC encipherment with PKCS7 padding of the plaintext using AES-128 with key “C5D3 …”; IV “vpSu….” produces:

```
252FCD2435FC78F7017B18C10C8699D3449CE53A99253DF602C6FB1826CCC1732023
B2702200435E326E9245F5EFB7D1C3DB170A3F9EC5E4461B6B829DCBAE0AA3693235
1E8AC62F126306D9F9167BECBB6869E7F3A7C7BD5C6C158FC001EC7ABFF36716FAD1
BA158609016C1D2FBD70CF2F7F816C952D43E319BF27A3DDDDD7AB3A86FEB8B96145
E6FC391F663202F5AFDF4B49BFCB1CF9969C0B8EB920F614594094EC6DCA65BE009D
00C6004FD907349DCF9EB069A2184E6098F5C6B8D5361B38EA584A415E1120954934
6EF73F6F54A20EF97DAD5C40947963EBE5FA8A1BAB5A0A1BC238EDDB6CC425A660C0
53F0A9C7FC7A20422BCECAF9F194358623630167 2F39021CA38F7FA3756E18288BB4
9B1E17BF2BEABA1FC672BBD2C3D6751AC303562DE84B31714ED62EE2F24D49711340
4D3A996D9F646E58B2808FE104BB2932F165D81823381450E985DA3ACC16A25344D4
44F9469D55C2F7E3BCFE7BC490B800308CDAB10EE153125EAB3CFBD7D7B96E85A9A7
C149803F8A524ED4385F63EF0EEB5BE1B2B100D709D7501B6E7BC90C578D7B559872
EDACBDFC2E51DBF4DF03C7AC81CE8DE43AA62F508E87169425AAC4B62003A19BE894
3FEB24B09195F6F35C3D52EB7A7210E4C6BF2B1DB8AE727D8F8F208B11D09FA71AE2
CC2377DB6A19E194BA1CF2F55D984C44C2E3CEFD1FEF49CF6AE71C9A777FE5B6DE81
417C69EA633F36EA69DA2556BA9E3393A6DDD5B5880ED9BECA8E18E59B34D2F15101
51D7282EDAE26C7B1DB5EA0175416103E152CA82D3BCFE63D627C8C618A0CE9ACAD3
A786784C380E7990A3469C841F042914642AE571AA2F70AF2E3C7A107F66EFEC67D0
D02D9DDC406506EF84DC6747CFEB8E370DD553F0BEF48801C262A0C438A42C746EEE
421C17F3214841434F563771A358B38A6BADEC1504AAADB897AC291C3FAB1D6DDA55
BCF277F15E973B4B194304C70C736C8A3F4C568E37B502333CCBBEE7623D91089CC0
63C60373B05D3653AF910B78605800788572E3F866DCDAFC6EC7EF9964413362FA41
E56C6DBDCAEE2C2E7CAE97ECA73C1F835A28F884AD073DA2F3780B6A1212409202E6
41671589AD158C01E83425E326969F3DDD0C39F92207D3FB40904A02820D6BE7F8D2
570B471D1C48B5F8E2819B14C524B9223496FF0FB2A6C469EABD1A656BABA47015B8
34F5BFC01097901308738B397E83789B66D5F0C33A900D38B8B12B7D7B0FE220AA92
555B6F6C4DFAD6DE03FFA127E035C4CE5E73889DD1582998D23D1961A3DE73DBE8AB
CA680BF379EE5FF0136083B1E63AF94BD746DCB215742ACA707E90B83C7E1417D58A
8682CCE9398C6F727168DD4758F6EE2E34325F025DF6B9F63F182D7DA6D9A0E72C50
D27D1D17AAE0DFD2886113CD26812FF666834A1AF8388D5F5B891780BCFA0A7497F5
179BCD70B19A916561BFC957BAD59520FDBB648E1A2ED751323216BE4F66DB0AB5F7
A8532C03E63333DEEB8E9D1977D6C0634A88FB74D4778815D865DF6A74734B5A28B5
FF6965C34B4C31ABC780EE35D08FDA107A705AFBAFC9C55CDE095463C0283CB2E72B
ECF58707FB84706C329EAB527D9270F99C7F09454B51FFFE11641A9A9C8FA1B43443
FC80DEEC0664C9A6C52E76F69A3D270DD8EAAE2C3F0955FAE4FF31BF64CA10971E48
27CAB6B61EC83F61A3FCB954CC7826B1802745E949108254D03D2946D34111520E86
26AFD60BFB3F62BAE6ADE3CD3941A59C859E7F291F5AA02D87F3C4CF8038E9C36266
C4F2E480F8344750AEBF1847F98C77D030045F584E9F81172D1D0A7FAC34AD4D6501
3B8CCA337C57CFB7AF6F0AB97AF6689FAEF19D9DC272D2B1A52C062A1772BA81D760
12C3
```

Base64url encoded:

```
JS_NJDX8ePcBexjBDIaZ00Sc5TqZJT32Asb7GCbMwXMgI7JwIgBDXjJukkX177fRw9sX
Cj-exeRGG2uCncuuCqNpMjUeisYvEmMG2fkWe-
y7aGnn86fHvVxsFY_AAex6v_NnFvrRuhWGCQFsHS-
9cM8vf4FslS1D4xm_J6Pd3derOob-
uLlhReb8OR9mMgL1r99LSb_LHPmWnAuOuSD2FFlAlOxtymW-AJ0AxgBP2Qc0nc-
esGmiGE5gmPXGuNU2GzjqWEpBXhEglUk0bvc_b1SiDvl9rVxAlHlj6-
X6ihurWgobwjjt22zEJaZgwFPwqcf8eiBCK87K-
fGUNYYjYwFnLzkCHKOPf6N1bhgoi7SbHhe_K-
q6H8Zyu9LD1nUawwNWLehLMXFO1i7i8k1JcRNATTqZbZ9kbliygI_hBLspMvFl2BgjOB
RQ6YXaOswWolNE1ET5Rp1VwvfjvP57xJC4ADCM2rEO4VMSXqs8-
9fXuW6FqafBSYA_ilJO1DhfY-
8O61vhsrEA1wnXUBtue8kMV417VZhy7ay9_C5R2_TfA8esgc6N5DqmL1COhxaUJarEti
ADoZvolD_rJLCRlfbzXD1S63pyEOTGvysduK5yfY-PIIsR0J-
nGuLMI3fbahnhlLoc8vVdmExEwuPO_R_vSc9q5xyad3_ltt6BQXxp6mM_Nupp2iVWup4
zk6bd1bWIDtm-yo4Y5Zs00vFRAVHXKC7a4mx7HbXqAXVBYQPhUsqC07z-
Y9YnyMYYoM6aytOnhnhMOA55kKNGnIQfBCkUZCrlcaovcK8uPHoQf2bv7GfQ0C2d3EBl
Bu-E3GdHz-uONw3VU_C-
9IgBwmKgxDikLHRu7kIcF_MhSEFDT1Y3caNYs4prrewVBKqtuJesKRw_qx1t2lW88nfx
Xpc7SxlDBMcMc2yKP0xWjje1AjM8y77nYj2RCJzAY8YDc7BdNlOvkQt4YFgAeIVy4_hm
3Nr8bsfvmWRBM2L6QeVsbb3K7iwufK6X7Kc8H4NaKPiErQc9ovN4C2oSEkCSAuZBZxWJ
rRWMAeg0JeMmlp893Qw5-SIH0_tAkEoCgg1r5_jSVwtHHRxItfjigZsUxSS5IjSW_w-
ypsRp6r0aZWurpHAVuDT1v8AQl5ATCHOLOX6DeJtm1fDDOpANOLixK317D-
IgqpJVW29sTfrW3gP_oSfgNcTOXnOIndFYKZjSPRlho95z2-
irymgL83nuX_ATYIOx5jr5S9dG3LIVdCrKcH6QuDx-
FBfVioaCzOk5jG9ycWjdR1j27i40Ml8CXfa59j8YLX2m2aDnLFDSfR0XquDf0ohhE80m
gS_2ZoNKGvg4jV9biReAvPoKdJf1F5vNcLGakWVhv8lXutWVIP27ZI4aLtdRMjIWvk9m
2wq196hTLAPmMzPe646dGXfWwGNKiPt01HeIFdhl32p0c0taKLX_aWXDS0wxq8eA7jXQ
j9oQenBa-6_JxVzeCVRjwCg8sucr7PWHB_uEcGwynqtSfZJw-Zx_CUVLUf_-
EWQampyPobQ0Q_yA3uwGZMmmxS529po9Jw3Y6q4sPwlV-
uT_Mb9kyhCXHkgnyra2Hsg_YaP8uVTMeCaxgCdF6UkQglTQPSlG00ERUg6GJq_WC_s_Y
rrmrePNOUGlnIWefykfWqAth_PEz4A46cNiZsTy5ID4NEdQrr8YR_mMd9AwBF9YTp-
BFy0dCn-sNK1NZQE7jMozfFfPt69vCrl69mifrvGdncJy0rGlLAYqF3K6gddgEsM
```

Authentication Tag

For the MAC, the Additional Authenticated Data (AAD) is the Protected Header, which in Hex of base64url string is

```
“65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636
D46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E4
351793149557A49314E694A39” so the AAD Length (AL) is
0000000000000280 (80 bytes = 640 bits).
```

The data to MAC is the concatenation of AAD (in ASCII), IV, Ciphertext and AL hence the data to MAC in hexadecimal is:

```
65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636D
46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E43
51793149557A49314E694A39
BE94AECB5F6706EE3BC88EAE1E5938A9
252FCD2435FC78F7017B18C10C8699D3449CE53A99253DF602C6FB1826CCC1732023
B2702200435E326E9245F5EFB7D1C3DB170A3F9EC5E4461B6B829DCBAE0AA3693235
1E8AC62F126306D9F9167BECBB6869E7F3A7C7BD5C6C158FC001EC7ABFF36716FAD1
BA158609016C1D2FBD70CF2F7F816C952D43E319BF27A3DDDDD7AB3A86FEB8B96145
E6FC391F663202F5AFDF4B49BFCB1CF9969C0B8EB920F614594094EC6DCA65BE009D
00C6004FD907349DCF9EB069A2184E6098F5C6B8D5361B38EA584A415E1120954934
6EF73F6F54A20EF97DAD5C40947963EBE5FA8A1BAB5A0A1BC238EDDB6CC425A660C0
53F0A9C7FC7A20422BCECAF9F194358623630167 2F39021CA38F7FA3756E18288BB4
9B1E17BF2BEABA1FC672BBD2C3D6751AC303562DE84B31714ED62EE2F24D49711340
4D3A996D9F646E58B2808FE104BB2932F165D81823381450E985DA3ACC16A25344D4
44F9469D55C2F7E3BCFE7BC490B800308CDAB10EE153125EAB3CFBD7D7B96E85A9A7
C149803F8A524ED4385F63EF0EEB5BE1B2B100D709D7501B6E7BC90C578D7B559872
EDACBDFC2E51DBF4DF03C7AC81CE8DE43AA62F508E87169425AAC4B62003A19BE894
3FEB24B09195F6F35C3D52EB7A7210E4C6BF2B1DB8AE727D8F8F208B11D09FA71AE2
CC2377DB6A19E194BA1CF2F55D984C44C2E3CEFD1FEF49CF6AE71C9A777FE5B6DE81
417C69EA633F36EA69DA2556BA9E3393A6DDD5B5880ED9BECA8E18E59B34D2F15101
51D7282EDAE26C7B1DB5EA0175416103E152CA82D3BCFE63D627C8C618A0CE9ACAD3
A786784C380E7990A3469C841F042914642AE571AA2F70AF2E3C7A107F66EFEC67D0
D02D9DDC406506EF84DC6747CFEB8E370DD553F0BEF48801C262A0C438A42C746EEE
421C17F3214841434F563771A358B38A6BADEC1504AAADB897AC291C3FAB1D6DDA55
BCF277F15E973B4B194304C70C736C8A3F4C568E37B502333CCBBEE7623D91089CC0
63C60373B05D3653AF910B78605800788572E3F866DCDAFC6EC7EF9964413362FA41
E56C6DBDCAEE2C2E7CAE97ECA73C1F835A28F884AD073DA2F3780B6A1212409202E6
41671589AD158C01E83425E326969F3DDD0C39F92207D3FB40904A02820D6BE7F8D2
570B471D1C48B5F8E2819B14C524B9223496FF0FB2A6C469EABD1A656BABA47015B8
34F5BFC01097901308738B397E83789B66D5F0C33A900D38B8B12B7D7B0FE220AA92
555B6F6C4DFAD6DE03FFA127E035C4CE5E73889DD1582998D23D1961A3DE73DBE8AB
CA680BF379EE5FF0136083B1E63AF94BD746DCB215742ACA707E90B83C7E1417D58A
8682CCE9398C6F727168DD4758F6EE2E34325F025DF6B9F63F182D7DA6D9A0E72C50
D27D1D17AAE0DFD2886113CD26812FF666834A1AF8388D5F5B891780BCFA0A7497F5
179BCD70B19A916561BFC957BAD59520FDBB648E1A2ED751323216BE4F66DB0AB5F7
A8532C03E63333DEEB8E9D1977D6C0634A88FB74D4778815D865DF6A74734B5A28B5
FF6965C34B4C31ABC780EE35D08FDA107A705AFBAFC9C55CDE095463C0283CB2E72B
ECF58707FB84706C329EAB527D9270F99C7F09454B51FFFE11641A9A9C8FA1B43443
FC80DEEC0664C9A6C52E76F69A3D270DD8EAAE2C3F0955FAE4FF31BF64CA10971E48
27CAB6B61EC83F61A3FCB954CC7826B1802745E949108254D03D2946D34111520E86
26AFD60BFB3F62BAE6ADE3CD3941A59C859E7F291F5AA02D87F3C4CF8038E9C36266
C4F2E480F8344750AEBF1847F98C77D030045F584E9F81172D1D0A7FAC34AD4D6501
3B8CCA337C57CFB7AF6F0AB97AF6689FAEF19D9DC272D2B1A52C062A1772BA81D760
12C3
0000000000000280
```

MACing using HMAC SHA256 and a key of "4B57…" produces:

```
6297EE493F75AC7F6E904387398A6044C49F49376978371E621F4E62B5B4664A
```

The most significant 16 bytes are the authentication tag which is

```
6297EE493F75AC7F6E904387398A6044
```

Base64url encoded

```
YpfuST91rH9ukEOHOYpgRA
```

Resulting JWE looks like

JWE Protected Header

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOENC
Qy1IUzI1NiJ9

.

.

vpSuy19nBu47yI6uHlk4qQ

.

JS_NJDX8ePcBexjBDIaZ00Sc5TqZJT32Asb7GCbMwXMgI7JwIgBDXjJukkX177fRw9sX
Cj-exeRGG2uCncuuCqNpMjUeisYvEmMG2fkWe-
y7aGnn86fHvVxsFY_AAex6v_NnFvrRuhWGCQFsHS-
9cM8vf4FslS1D4xm_J6Pd3derOob-
uLlhReb8OR9mMgL1r99LSb_LHPmWnAuOuSD2FFlAlOxtymW-AJ0AxgBP2Qc0nc-
esGmiGE5gmPXGuNU2GzjqWEpBXhEglUk0bvc_b1SiDvl9rVxAlHlj6-
X6ihurWgobwjjt22zEJaZgwFPwqcf8eiBCK87K-
fGUNYYjYwFnLzkCHKOPf6N1bhgoi7SbHhe_K-
q6H8Zyu9LD1nUawwNWLehLMXFO1i7i8k1JcRNATTqZbZ9kbliygI_hBLspMvFl2BgjOB
RQ6YXaOswWolNE1ET5Rp1VwvfjvP57xJC4ADCM2rEO4VMSXqs8-
9fXuW6FqafBSYA_ilJO1DhfY-
8O61vhsrEA1wnXUBtue8kMV417VZhy7ay9_C5R2_TfA8esgc6N5DqmL1COhxaUJarEti
ADoZvolD_rJLCRlfbzXD1S63pyEOTGvysduK5yfY-PIIsR0J-
nGuLMI3fbahnhlLoc8vVdmExEwuPO_R_vSc9q5xyad3_ltt6BQXxp6mM_Nupp2iVWup4
zk6bd1bWIDtm-yo4Y5Zs00vFRAVHXKC7a4mx7HbXqAXVBYQPhUsqC07z-
Y9YnyMYYoM6aytOnhnhMOA55kKNGnIQfBCkUZCrlcaovcK8uPHoQf2bv7GfQ0C2d3EBl
Bu-E3GdHz-uONw3VU_C-
9IgBwmKgxDikLHRu7kIcF_MhSEFDT1Y3caNYs4prrewVBKqtuJesKRw_qx1t2lW88nfx
Xpc7SxlDBMcMc2yKP0xWjje1AjM8y77nYj2RCJzAY8YDc7BdNlOvkQt4YFgAeIVy4_hm
3Nr8bsfvmWRBM2L6QeVsbb3K7iwufK6X7Kc8H4NaKPiErQc9ovN4C2oSEkCSAuZBZxWJ
rRWMAeg0JeMmlp893Qw5-SIH0_tAkEoCgg1r5_jSVwtHHRxItfjigZsUxSS5IjSW_w-
ypsRp6r0aZWurpHAVuDT1v8AQl5ATCHOLOX6DeJtm1fDDOpANOLixK317D-
IgqpJVW29sTfrW3gP_oSfgNcTOXnOIndFYKZjSPRlho95z2-
irymgL83nuX_ATYIOx5jr5S9dG3LIVdCrKcH6QuDx-
FBfVioaCzOk5jG9ycWjdR1j27i40Ml8CXfa59j8YLX2m2aDnLFDSfR0XquDf0ohhE80m
gS_2ZoNKGvg4jV9biReAvPoKdJf1F5vNcLGakWVhv8lXutWVIP27ZI4aLtdRMjIWvk9m
2wq196hTLAPmMzPe646dGXfWwGNKiPt01HeIFdhl32p0c0taKLX_aWXDS0wxq8eA7jXQ
j9oQenBa-6_JxVzeCVRjwCg8sucr7PWHB_uEcGwynqtSfZJw-Zx_CUVLUf_-
EWQampyPobQ0Q_yA3uwGZMmmxS529po9Jw3Y6q4sPwlV-
uT_Mb9kyhCXHkgnyra2Hsg_YaP8uVTMeCaxgCdF6UkQglTQPSlG00ERUg6GJq_WC_s_Y
rrmrePNOUGlnIWefykfWqAth_PEz4A46cNiZsTy5ID4NEdQrr8YR_mMd9AwBF9YTp-
BFy0dCn-sNK1NZQE7jMozfFfPt69vCrl69mifrvGdncJy0rGlLAYqF3K6gddgEsM

.

YpfuST91rH9ukEOHOYpgRA
```

SDK Decryption

The SDK unwraps the protected header to yield this

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128CBC-HS256"}
```

From which it understands that it must use AES 128 bit CBC with HMAC-256.

It determines the binary version of the protected header as

```
65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636D
46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E43
51793149557A49314E694A39
```

From which it determines the bitlength as 640 bits and AL as `0000000000000280`

The data to HMAC with key “4B57….” is therefore:

```
65794A68624763694F694A6B615849694C434A72615751694F694A4251314E55636D
46756332466A64476C76626B6C45496977695A57356A496A6F69515445794F454E43
51793149557A49314E694A39
BE94AECB5F6706EE3BC88EAE1E5938A9
252FCD2435FC78F7017B18C10C8699D3449CE53A99253DF602C6FB1826CCC1732023
B2702200435E326E9245F5EFB7D1C3DB170A3F9EC5E4461B6B829DCBAE0AA3693235
1E8AC62F126306D9F9167BECBB6869E7F3A7C7BD5C6C158FC001EC7ABFF36716FAD1
BA158609016C1D2FBD70CF2F7F816C952D43E319BF27A3DDDDD7AB3A86FEB8B96145
E6FC391F663202F5AFDF4B49BFCB1CF9969C0B8EB920F614594094EC6DCA65BE009D
00C6004FD907349DCF9EB069A2184E6098F5C6B8D5361B38EA584A415E1120954934
6EF73F6F54A20EF97DAD5C40947963EBE5FA8A1BAB5A0A1BC238EDDB6CC425A660C0
53F0A9C7FC7A20422BCECAF9F1943586236301672F39021CA38F7FA3756E18288BB4
9B1E17BF2BEABA1FC672BBD2C3D6751AC303562DE84B31714ED62EE2F24D49711340
4D3A996D9F646E58B2808FE104BB2932F165D81823381450E985DA3ACC16A25344D4
44F9469D55C2F7E3BCFE7BC490B800308CDAB10EE153125EAB3CFBD7D7B96E85A9A7
C149803F8A524ED4385F63EF0EEB5BE1B2B100D709D7501B6E7BC90C578D7B559872
EDACBDFC2E51DBF4DF03C7AC81CE8DE43AA62F508E87169425AAC4B62003A19BE894
3FEB24B09195F6F35C3D52EB7A7210E4C6BF2B1DB8AE727D8F8F208B11D09FA71AE2
CC2377DB6A19E194BA1CF2F55D984C44C2E3CEFD1FEF49CF6AE71C9A777FE5B6DE81
417C69EA633F36EA69DA2556BA9E3393A6DDD5B5880ED9BECA8E18E59B34D2F15101
51D7282EDAE26C7B1DB5EA0175416103E152CA82D3BCFE63D627C8C618A0CE9ACAD3
A786784C380E7990A3469C841F042914642AE571AA2F70AF2E3C7A107F66EFEC67D0
D02D9DDC406506EF84DC6747CFEB8E370DD553F0BEF48801C262A0C438A42C746EEE
421C17F3214841434F563771A358B38A6BADEC1504AAADB897AC291C3FAB1D6DDA55
BCF277F15E973B4B194304C70C736C8A3F4C568E37B502333CCBBEE7623D91089CC0
63C60373B05D3653AF910B78605800788572E3F866DCDAFC6EC7EF9964413362FA41
E56C6DBDCAEE2C2E7CAE97ECA73C1F835A28F884AD073DA2F3780B6A1212409202E6
41671589AD158C01E83425E326969F3DDD0C39F92207D3FB40904A02820D6BE7F8D2
570B471D1C48B5F8E2819B14C524B9223496FF0FB2A6C469EABD1A656BABA47015B8
34F5BFC01097901308738B397E83789B66D5F0C33A900D38B8B12B7D7B0FE220AA92
555B6F6C4DFAD6DE03FFA127E035C4CE5E73889DD1582998D23D1961A3DE73DBE8AB
CA680BF379EE5FF0136083B1E63AF94BD746DCB215742ACA707E90B83C7E1417D58A
8682CCE9398C6F727168DD4758F6EE2E34325F025DF6B9F63F182D7DA6D9A0E72C50
D27D1D17AAE0DFD2886113CD26812FF666834A1AF8388D5F5B891780BCFA0A7497F5
179BCD70B19A916561BFC957BAD59520FDBB648E1A2ED751323216BE4F66DB0AB5F7
A8532C03E63333DEEB8E9D1977D6C0634A88FB74D4778815D865DF6A74734B5A28B5
FF6965C34B4C31ABC780EE35D08FDA107A705AFBAFC9C55CDE095463C0283CB2E72B
ECF58707FB84706C329EAB527D9270F99C7F09454B51FFFE11641A9A9C8FA1B43443
FC80DEEC0664C9A6C52E76F69A3D270DD8EAAE2C3F0955FAE4FF31BF64CA10971E48
27CAB6B61EC83F61A3FCB954CC7826B1802745E949108254D03D2946D3411520E86
```

```
26AFD60BFB3F62BAE6ADE3CD3941A59C859E7F291F5AA02D87F3C4CF8038E9C36266
C4F2E480F8344750AEBF1847F98C77D030045F584E9F81172D1D0A7FAC34AD4D6501
3B8CCA337C57CFB7AF6F0AB97AF6689FAEF19D9DC272D2B1A52C062A1772BA81D760
12C3
0000000000000280
```

Giving the hash result

```
6297EE493F75AC7F6E904387398A6044
```

Base64url encoded

```
YpfuST91rH9ukEOHOYpgRA
```

Which matches the token in the message

The SDK decrypts the message “JS_N…”

using IV “vpSu…”

using key C5D3…

Decrypted Value

CBC decipherment of message “JS_N…”using AES-128 with key “C5D3…”; IV “vpSu….” produces:

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","uiType":"01","challengeAddInfo":"Additional
information to be shown.",
"challengeCompletionInd":"N","challengeInfoHeader":"Header
information","challengeInfoLabel":"One-time-
password","challengeInfoText":"Please enter the received one-time-
password","challengeInfoTextIndicator":"N","expandInfoLabel1":"Addit
ional instructions","expandInfoText1":"The issuer will send you via
SMS a one-time password. Please enter the value in the designated
input field above and press continue to complete the 3-D Secure
authentication
process.","issuerImage":{"medium":"http://acs.com/medium_image.svg",
"high":"http://acs.com/high_image.svg","extraHigh":"http://acs.com/e
xtraHigh_image.svg"},"messageType":"CRes","messageVersion":"2.1.0","
psImage":
{"medium":"http://ds.com/medium_image.svg","high":"http://ds.com/hig
h_image.svg","extraHigh":"http://ds.com/extraHigh_image.svg"},"resen
dInformationLabel":"Send new One-time-
password","sdkTransID":"b2385523-a66c-4907-ac3c-
91848e8c0067","submitAuthenticationLabel":"Continue","whyInfoLabel1"
:"Why using 3-D Secure?","whyInfoText1":"Some explanation about why
using 3-D Secure is an excellent idea as part of an online payment
transaction","acsCounterAtoS":"001"}
```

ACS Encryption of CRes and SDK Decryption—Using A128GCM

CRes Message Contents

Plaintext Data

```
{
"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-b08d1690b26e",
"acsTransID":"d7c1ee99-9478-44a6-b1f2-391e29c6b340",
"uiType":"01",
"challengeAddInfo":"Additional information to be shown.",
"challengeCompletionInd":"N",
"challengeInfoHeader":"Header information",
"challengeInfoLabel":"One-time-password",
"challengeInfoText":"Please enter the received one-time-password",
"challengeInfoTextIndicator":"N",
"expandInfoLabel1":"Additional instructions",
"expandInfoText1":"The issuer will send you via SMS a one-time
password. Please enter the value in the designated input field above
and press continue to complete the 3-D Secure authentication
process.",
"issuerImage":{
      "medium":"http://acs.com/medium_image.svg",
      "high":"http://acs.com/high_image.svg",
      "extraHigh":"http://acs.com/extraHigh_image.svg"
},
"messageType":"CRes",
"messageVersion":"2.1.0",
"psImage": {
      "medium":"http://ds.com/medium_image.svg",
      "high":"http://ds.com/high_image.svg",
      "extraHigh":"http://ds.com/extraHigh_image.svg"
},
"resendInformationLabel":"Send new One-time-password",
"sdkTransID":"b2385523-a66c-4907-ac3c-91848e8c0067",
"submitAuthenticationLabel":"Continue",
"whyInfoLabel1":"Why using 3-D Secure?",
"whyInfoText1":"Some explanation about why using 3-D Secure is an
excellent idea as part of an online payment transaction",
"acsCounterAtoS":"001"
}
```

Without whitespace

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","uiType":"01","challengeAddInfo":"Additional
information to be shown.",
"challengeCompletionInd":"N","challengeInfoHeader":"Header
information","challengeInfoLabel":"One-time-
password","challengeInfoText":"Please enter the received one-time-
password","challengeInfoTextIndicator":"N","expandInfoLabel1":"Addit
ional instructions","expandInfoText1":"The issuer will send you via
SMS a one-time password. Please enter the value in the designated
input field above and press continue to complete the 3-D Secure
authentication
process.","issuerImage":{"medium":"http://acs.com/medium_image.svg",
"high":"http://acs.com/high_image.svg","extraHigh":"http://acs.com/e
xtraHigh_image.svg"},"messageType":"CRes","messageVersion":"2.1.0","
psImage":
{"medium":"http://ds.com/medium_image.svg","high":"http://ds.com/hig
h_image.svg","extraHigh":"http://ds.com/extraHigh_image.svg"},"resen
dInformationLabel":"Send new One-time-
password","sdkTransID":"b2385523-a66c-4907-ac3c-
91848e8c0067","submitAuthenticationLabel":"Continue","whyInfoLabel1"
:"Why using 3-D Secure?","whyInfoText1":"Some explanation about why
using 3-D Secure is an excellent idea as part of an online payment
transaction","acsCounterAtoS":"001"}
```

CEK from previous DH exchange is the rightmost half of the derived key:

```
C5D37C30CBEF51D4642A8D1BB22A1C23
```

Initialization Vector

For GCM mode the IV is the counter left padded with FF bytes.

The counter is a 1 byte counter and in this example is "001", so the IV would be

FFFFFFFFFFFFFFFFFFFFFF01

which in base64url format is

______________8B

Protected Header

```
{
     "alg":”dir",
     “kid”:”ACSTransactionID”,
     "enc":”A128GCM"
}
```

Without whitespace

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128GCM"}
```

BASE64url encoded

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOEdD
TSJ9
```

Data Encipherment

GCM encipherment of the plaintext using AES-128 with key “C5D3…”; IV “__...8B”; Protected Header “eyJh…”produces:

```
F39AF457AFFF2A1C4DA1A56BFD91CB47A4F5635007F1A6589A7902B1A0DAC1E45AA6
1503E08CC994A83805581EEA4C2824BADF329FDEA87420119ED2FD5C48E29F06FC8A
AC7D5A2DC7BF4549141805D40ABD0A593F21264958BFB6381BBF3DB4042D3747B18F
E94414F3550711D40E89AA01F00639F1F0E5EB22921B9F487FFDF910ACB9FAB37DC1
671442ACEBB4057DD784C8446226E0427ECE2B77D0C6B574800E858EAAFCDACA4534
A9473233346BF809DBDF66372FA8A0F984B12297413813D93B7D9E6C8CEBE27B9DDF
3BE426F319DE825432FCC1EFE21ABE8195B6FC6E91F017AC9AB678F31CCCEEFAD389
62E619671047F4ED85EF7864BDA0AA12F7DA58B01FC669D718AE1EB3A308397F12A6
A4BD7E4C183696573A0A8EBD743EE9FC4F314AF57DCEFEE9079FCEE91940B3D50F66
92D455321AFF24282D2FB02E69D0CDA702D3886C9C186064F17FB31DA60DDFEFA018
EC7AE880098342754C779D564786179188BCDAA8D29985DD7303CF71FB62B5FB1AC3
8005FD7D8A678E222826D025CE105489CD8B128F0A7F93D01EA6635F837259B746E4
F583DF43B2E256AD6BB36390FFA88AFCC761E1DB31D8077276B3A485CC10E6EEEB06
41A6DD3B5A1CD27C7E3D15D8C0FB30513E41CBD3CF986DD3EB030A72CD7AE8259E35
E5157867C3871A8A6F4CE62243F535B7ACC55CDA7D57DF0E1F054B8E951D9C726C96
C534D330B08842775779D41D1B7ED055BC7432559E8F3570567FB79E9EF3F01F12C1
421D9EA66570380F0B738AB335E97AA26B1F77F6BB0A93724B2024034CAC698BA6FB
62B2FBEFE9560A57D747F48D9F7D4D5E53FD828DAF71A5296E0FC3B9BAF8E76D25C6
F956BCF906CB1A8C9BF44054B4A3458404E3FA6E3957F03B3E5DD00869659D15E2E8
7864ED388A71D4790A6E9E50ACBF6A4081A48E1CB0EFBA46508B055F625B587AAA10
5A6E4CBBE249B4C8389DCC108A85DD15F3F7D74D16C84F3B3DB1E75961822645134E
B13E2EC5177120E0C163BB7464F93CED237E5D9B572AE2DB769BF1A073519A50EA1E
8EC95ECAEF2F6D882B5B3EABA5AB180B238C8CE66FBB9512A66C5467DAA489D64187
371F3C81BE14ACBA8EE6EE14BC0BF2892D499F5398F76E038604EFCCF89AC52B8410
8233565DFF335A36D6E917246C3977105DE09EF724F4459362777DB15CFC61B6822A
F27C7E1212E248EFF2A9AEB08B4AB8A571A9F0EA71FE6BF1874F43A83A5A4B7E528C
F0394342987571F3BBEEDC12F8CE971BD90DE82975A1B582F2AC3D8AE4E04198A639
78177B55C15E4AA3B4CEB311BBAC062CBF83CFF1D191231B7F57EC27254946FA540B
3BDFCE4B25E865C26B107E1D295583E76EE3AE9661F511F6E966DA6B21C99BCF9933
5898C6C4FEAD1E43DDE6F5B4566B395716589363660D5C26B9B87EEFEB7707211BC7
DEEC0F609124870CF1DA9A299B8C3C0F3A35D70EBA965C0F5E1F8732A16AF475C182
A1C1338ECA6AA05A4F3566E98617853B89A1563B38DDA147D60AC45E928B0F9AF930
11B566B27E92D9B8DD26C4EDE644C01A447808F65CA829898B4C7885A9BF3E624DBB
F68C0EE79E49970BD9468A2CF7A5A60FC47C4400A8EB5FCC5EBA219F741F734FC0FF
33DCA741F42ADB6762778E20D9CA2F8E543065A946825DFE251F47A10877549D25DF
1BF571486DE253E03701CCFB846D32A0192AD79EEE3126531C5D36D4B9F36434A287
29CE63BEF069A75C3ADDDA7EE1FA3AEBBC75801EF91E22A7FAD80D468C78DE534042
545E9F8ACB6F796270CF8305D807B99B4F596BB473750D206FEE8CC9FC577B2B20C7
E36E2E8B47234180CC481219C1B404983EE717D7
```

Base64url encoded:

```
85r0V6__KhxNoaVr_ZHLR6T1Y1AH8aZYmnkCsaDaweRaphUD4IzJlKg4BVge6kwoJLrf
Mp_eqHQgEZ7S_VxI4p8G_IqsfVotx79FSRQYBdQKvQpZPyEmSVi_tjgbvz20BC03R7GP
6UQU81UHEdQOiaoB8AY58fDl6yKSG59If_35EKy5-rN9wWcUQqzrtAV914TIRGIm4EJ-
zit30Ma1dIAOhY6q_NrKRTSpRzIzNGv4CdvfZjcvqKD5hLEil0E4E9k7fZ5sjOvie53f
O-Qm8xneglQy_MHv4hq-
gZW2_G6R8BesmrZ48xzM7vrTiWLmGWcQR_Tthe94ZL2gqhL32liwH8Zp1xiuHrOjCDl_
EqakvX5MGDaWVzoKjr10Pun8TzFK9X3O_ukHn87pGUCz1Q9mktRVMhr_JCgtL7AuadDN
pwLTiGycGGBk8X-zHaYN3--
gGOx66IAJg0J1THedVkeGF5GIvNqo0pmF3XMDz3H7YrX7GsOABf19imeOIigm0CXOEFS
JzYsSjwp_k9AepmNfg3JZt0bk9YPfQ7LiVq1rs2OQ_6iK_Mdh4dsx2AdydrOkhcwQ5u7
rBkGm3TtaHNJ8fj0V2MD7MFE-QcvTz5ht0-
sDCnLNeuglnjXlFXhnw4caim9M5iJD9TW3rMVc2n1X3w4fBUuOlR2ccmyWxTTTMLCIQn
dXedQdG37QVbx0MlWejzVwVn-
3np7z8B8SwUIdnqZlcDgPC3OKszXpeqJrH3f2uwqTcksgJANMrGmLpvtisvvv6VYKV9d
H9I2ffU1eU_2Cja9xpSluD8O5uvjnbSXG-Va8-QbLGoyb9EBUtKNFhATj-
m45V_A7Pl3QCGllnRXi6Hhk7TiKcdR5Cm6eUKy_akCBpI4csO-
6RlCLBV9iW1h6qhBabky74km0yDidzBCKhd0V8_fXTRbITzs9sedZYYImRRNOsT4uxRd
xIODBY7t0ZPk87SN-XZtXKuLbdpvxoHNRmlDqHo7JXsrvL22IK1s-
q6WrGAsjjIzmb7uVEqZsVGfapInWQYc3HzyBvhSsuo7m7hS8C_KJLUmfU5j3bgOGBO_M
-
JrFK4QQgjNWXf8zWjbW6RckbDl3EF3gnvck9EWTYnd9sVz8YbaCKvJ8fhIS4kjv8qmus
ItKuKVxqfDqcf5r8YdPQ6g6Wkt-
UozwOUNCmHVx87vu3BL4zpcb2Q3oKXWhtYLyrD2K5OBBmKY5eBd7VcFeSqO0zrMRu6wG
LL-Dz_HRkSMbf1fsJyVJRvpUCzvfzksl6GXCaxB-HSlVg-
du466WYfUR9ulm2mshyZvPmTNYmMbE_q0eQ93m9bRWazlXFliTY2YNXCa5uH7v63cHIR
vH3uwPYJEkhwzx2popm4w8Dzo11w66llwPXh-
HMqFq9HXBgqHBM47KaqBaTzVm6YYXhTuJoVY7ON2hR9YKxF6Siw-a-
TARtWayfpLZuN0mxO3mRMAaRHgI9lyoKYmLTHiFqb8-
Yk279owO555JlwvZRoos96WmD8R8RACo61_MXrohn3Qfc0_A_zPcp0H0KttnYneOINnK
L45UMGWpRoJd_iUfR6EId1SdJd8b9XFIbeJT4DcBzPuEbTKgGSrXnu4xJlMcXTbUufNk
NKKHKc5jvvBpp1w63dp-4fo667x1gB75HiKn-tgNRox43lNAQlRen4rLb3licM-
DBdgHuZtPWWu0c3UNIG_ujMn8V3srIMfjbi6LRyNBgMxIEhnBtASYPucX1w
```

Authentication Tag

```
CA3F15ABD5192A86352CBD7D835B339D
```

Base64url encoded:

```
yj8Vq9UZKoY1LL19g1sznQ
```

Resulting JWE looks like

JWE Protected Header

Initialization Vector

Ciphertext

Authentication Tag

In Compact Serialization

```
eyJhbGciOiJkaXIiLCJraWQiOiJBQ1NUcmFuc2FjdGlvbklEIiwiZW5jIjoiQTEyOEdD
TSJ9

.

.

______________8B

.

85r0V6__KhxNoaVr_ZHLR6T1Y1AH8aZYmnkCsaDaweRaphUD4IzJlKg4BVge6kwoJLrf
Mp_eqHQgEZ7S_VxI4p8G_IqsfVotx79FSRQYBdQKvQpZPyEmSVi_tjgbvz20BC03R7GP
6UQU81UHEdQOiaoB8AY58fDl6yKSG59If_35EKy5-rN9wWcUQqzrtAV914TIRGIm4EJ-
zit30Ma1dIAOhY6q_NrKRTSpRzIzNGv4CdvfZjcvqKD5hLEil0E4E9k7fZ5sjOvie53f
O-Qm8xneglQy_MHv4hq-
gZW2_G6R8BesmrZ48xzM7vrTiWLmGWcQR_Tthe94ZL2gqhL32liwH8Zp1xiuHrOjCDl_
EqakvX5MGDaWVzoKjr10Pun8TzFK9X3O_ukHn87pGUCz1Q9mktRVMhr_JCgtL7AuadDN
pwLTiGycGGBk8X-zHaYN3--
gGOx66IAJg0J1THedVkeGF5GIvNqo0pmF3XMDz3H7YrX7GsOABf19imeOIigm0CXOEFS
JzYsSjwp_k9AepmNfg3JZt0bk9YPfQ7LiVq1rs2OQ_6iK_Mdh4dsx2AdydrOkhcwQ5u7
rBkGm3TtaHNJ8fj0V2MD7MFE-QcvTz5ht0-
sDCnLNeuglnjXlFXhnw4caim9M5iJD9TW3rMVc2n1X3w4fBUuOlR2ccmyWxTTTMLCIQn
dXedQdG37QVbx0MlWejzVwVn-
3np7z8B8SwUIdnqZlcDgPC3OKszXpeqJrH3f2uwqTcksgJANMrGmLpvtisvvv6VYKV9d
H9I2ffU1eU_2Cja9xpSluD8O5uvjnbSXG-Va8-QbLGoyb9EBUtKNFhATj-
m45V_A7Pl3QCGllnRXi6Hhk7TiKcdR5Cm6eUKy_akCBpI4csO-
6RlCLBV9iW1h6qhBabky74km0yDidzBCKhd0V8_fXTRbITzs9sedZYYImRRNOsT4uxRd
xIODBY7t0ZPk87SN-XZtXKuLbdpvxoHNRmlDqHo7JXsrvL22IK1s-
q6WrGAsjjIzmb7uVEqZsVGfapInWQYc3HzyBvhSsuo7m7hS8C_KJLUmfU5j3bgOGBO_M
-
JrFK4QQgjNWXf8zWjbW6RckbDl3EF3gnvck9EWTYnd9sVz8YbaCKvJ8fhIS4kjv8qmus
ItKuKVxqfDqcf5r8YdPQ6g6Wkt-
UozwOUNCmHVx87vu3BL4zpcb2Q3oKXWhtYLyrD2K5OBBmKY5eBd7VcFeSqO0zrMRu6wG
LL-Dz_HRkSMbf1fsJyVJRvpUCzvfzksl6GXCaxB-HSlVg-
du466WYfUR9ulm2mshyZvPmTNYmMbE_q0eQ93m9bRWazlXFliTY2YNXCa5uH7v63cHIR
vH3uwPYJEkhwzx2popm4w8Dzo11w66llwPXh-
HMqFq9HXBgqHBM47KaqBaTzVm6YYXhTuJoVY7ON2hR9YKxF6Siw-a-
TARtWayfpLZuN0mxO3mRMAaRHgI9lyoKYmLTHiFqb8-
Yk279owO555JlwvZRoos96WmD8R8RACo61_MXrohn3Qfc0_A_zPcp0H0KttnYneOINnK
L45UMGWpRoJd_iUfR6EId1SdJd8b9XFIbeJT4DcBzPuEbTKgGSrXnu4xJlMcXTbUufNk
NKKHKc5jvvBpp1w63dp-4fo667x1gB75HiKn-tgNRox43lNAQlRen4rLb3licM-
DBdgHuZtPWWu0c3UNIG_ujMn8V3srIMfjbi6LRyNBgMxIEhnBtASYPucX1w

.

yj8Vq9UZKoY1LL19g1sznQ
```

SDK Decryption

The SDK unwraps the protected header to yield this

```
{"alg":"dir","kid":"ACSTransactionID","enc":"A128GCM"}
```

From which it understands that it must use AES 128 bit GCM.

GCM decipherment of the message “85r0…” using Additional Authenticated Data “eyJh…”; IV “__...8B”; Authentication Tag “yj8V…”; key ”C5D3…“ produces:

```
{"threeDSServerTransID":"8a880dc0-d2d2-4067-bcb1-
b08d1690b26e","acsTransID":"d7c1ee99-9478-44a6-b1f2-
391e29c6b340","uiType":"01","challengeAddInfo":"Additional
information to be shown.",
"challengeCompletionInd":"N","challengeInfoHeader":"Header
information","challengeInfoLabel":"One-time-
password","challengeInfoText":"Please enter the received one-time-
password","challengeInfoTextIndicator":"N","expandInfoLabel1":"Addit
ional instructions","expandInfoText1":"The issuer will send you via
SMS a one-time password. Please enter the value in the designated
input field above and press continue to complete the 3-D Secure
authentication
process.","issuerImage":{"medium":"http://acs.com/medium_image.svg",
"high":"http://acs.com/high_image.svg","extraHigh":"http://acs.com/e
xtraHigh_image.svg"},"messageType":"CRes","messageVersion":"2.1.0","
psImage":
{"medium":"http://ds.com/medium_image.svg","high":"http://ds.com/hig
h_image.svg","extraHigh":"http://ds.com/extraHigh_image.svg"},"resen
dInformationLabel":"Send new One-time-
password","sdkTransID":"b2385523-a66c-4907-ac3c-
91848e8c0067","submitAuthenticationLabel":"Continue","whyInfoLabel1"
:"Why using 3-D Secure?","whyInfoText1":"Some explanation about why
using 3-D Secure is an excellent idea as part of an online payment
transaction","acsCounterAtoS":"001"}
```