



EMVCo Terminal Config  
For EMV 4.3e

Version 4.3e

Date: November 2015

# **Contents**

**References**

**Brief Description**

**Terminal Configuration**

**Key Data**

## **Brief Description**

The following pages shows each ICCSim script with the corresponding EMVCo test script. The description will show if the test script needs any specific conditions i.e. a specific amount or card to be used.

## ***PIN Values***

In the majority of tests if a PIN is to be entered this can be any value. If a specific value is needed it will be mentioned next to the test.

## ***Tool Version***

ICCSimTMat should be used for testing

## ***Card Versions***

A v7.35 card is used for all the tests in this document except for the T=1 tests which need v736

Tool will prompt for correct version and also download the applet if needed

The card version will be displayed in the log

## ***Magnetic Stripe Track 2 data***

The T=1 card has a track 2 on the magnetic stripe with a '601' service code whereas the

## ***Terminal Configuration***

Please see the next section

## Card Acceptance Device Configuration

The following AIDs need to be configured on the Card Acceptance Device for testing:

Visa AID: **A0000000031010**  
 Non-EMV AID: **A0000000999090**  
 Test **A00000999901**  
 ANO3 **A000000003101003**  
 ANO4 **A000000003101004**  
 ANO5 **A000000003101005**  
 ANO6 **A000000003101006**

**A000000003101007**

The Application Selection Indicator should be set to only one occurrence for this AID - all other AIDs should allow partial matching

### ANO7

Mastercard AID **A0000000041010**  
 JCB AID **A0000000651010**  
 AMEX AID **A000000025010501**  
 Discover AID **A0000001523010**  
 CUP AID **A000000333010102**

ANOD **A122334455**  
 ANOE **A0000000031010010203040506070809**

The following CA Public Keys need to be loaded onto the Card Acceptance Device (see following section for values):

**CA Index '54' '96' '57' '50' '51' '58' and '53' for RID 'A000000003'**

**E1' 'E2' 'E3' 'E4' 'E5' 'E6' for RID 'A000009999'**

**FA', 'FB', 'FC', 'FD', 'FE' and 'FF' for RID 'A000000004'**

**'02' and '03' for RID 'A000000065'**

**'60' and '61' for RID 'A000000025'**

**'C0' and 'C1' for RID 'A000000333'**

**'D0' and 'D1' for RID 'A000000152'**

For the following AIDS the following data must be configured:

**A0000000031010**

Data	Data for test ca.124.00 - if different from default
------	---

<b>9F01 Acquirer Identifier</b>	01234567891	Same
<b>9F09 Application Version Number</b>	0096	Same

<b>Merchant Category Code 9F15</b>	1234 30303030303030303030303030303030	Same
<b>Merchant Identifier 9F16</b>	0303030	Same
<b>Merchant Name and Location</b>	53484F502031 (SHOP 1)	Same
<b>TACs</b>	All zero unless test case specifies 150 unless test case specifies	Same - all zero
<b>Terminal Floor limit</b>	specifies	Same - 150
<b>Terminal Identification 9F1C</b>	46726F6E74202020	Same
<b>Transaction Currency Code 5F2A</b>	0840	Same
<b>Transaction Currency Exponent 5F36</b>	02	02
<b>Transaction Reference currency code 9F3C</b>	0840	0840
<b>Transaction Reference currency exponent</b>	02	02
<b>Terminal Risk Management Data 9F1D</b>	{Empty}	01

**A0000000041010**

<b>9F01 Acquirer Identifier</b>	01225566334	Same
<b>9F09 Application Version Number</b>	0002	Same
<b>Merchant Category Code 9F15</b>	1342 30303030303030303030303030303030	Same
<b>Merchant Identifier 9F16</b>	0303131	Same
<b>Merchant Name and Location</b>	SHOP 2	Same
<b>TACs</b>	All zero unless test case specifies 150 unless test case specifies	Dafault and Online are all zero and Denial is 4000000000
<b>Terminal Floor limit</b>	specifies	200 - change back after test
<b>Terminal Identification 9F1C</b>	4261636B20202020	Same
<b>Transaction Currency Code 5F2A</b>	0840	0056
<b>Transaction Currency Exponent 5F36</b>	{Empty}	3
<b>Transaction Reference currency code 9F3C</b>	{Empty}	0056
<b>Transaction Reference currency exponent</b>	{Empty}	3
<b>Terminal Risk Management Data 9F1D</b>	{Empty}	02

**A0000000651010**





<b>Transaction Currency Code 5F2A</b>	0840	0156
<b>Transaction Currency Exponent 5F36</b>	{Empty}	6
<b>Transaction Reference currency code 9F3C</b>	{Empty}	0156
<b>Transaction Reference currency exponent</b>	{Empty}	6
<b>Terminal Risk Management Data 9F1D</b>		
	{Empty}	06

The **Application Version Number** Stored on the Card Acceptance Device should be:

<b>'0096'</b>	For Visa (A000000003)
0001'	For AMEX (A000000025)
0002'	For MasterCard (A000000004)
0200'	For JCB (A000000065)
0030'	For CUP (A000000333)
0001'	For Discover (A000000152)
0009'	For Test App (A000000099)
9999'	For 2nd Test App (A000009999)
1234'	For ANOD (A122334455)

The **Terminal Country Code** should be set to:

**'0840'**

**Terminal Floor limit should be 150**

**DDOL** should be set to '9F37'

Unless specified in the test case the **Terminal Action Codes** should be set to '00000000'

**IFD Serial Number (9F1E)**

5465726D696E616C0000

**Merchant Identifier (9F16)**

30303030303030303030303030303030

**Certification Revocation Lists (utilised when the test requires a revocation list)**

For each of the RIDs	A000000003'
	A000000004'
	A000009999'

There needs to be 30 CRL entries (29 can contain Certificate Serial Numbers which are not signed i.e. dummy test data, see test cc.023)

For RID **'A000000003'** the signed CRL entry is for:

- CA Index '50'
- Certificate Serial Number '014455'



For RID '**A000000004**' the signed CRL entry is for:

- CA Index 'FE'
- Certificate Serial Number '092355'

For RID '**A000009999**' the signed CRL entry is for:

- CA Index 'E1'
- Certificate Serial Number '014394'

Default host message contains issuer authentication of 10 bytes - 8 byte ARPC and 2 byte response code 3030

Test will define if different or see ICCSim50\Documents - ICCSimTMat EMVL2 v4xx









0'

# Test Certificate Authority Public Keys For RID 'A000009999'

Please note that the Hash mentioned in all the key values below uses the CA Public Key Index. If you require another index to be used please contact [support@iccsolutions.com](mailto:support@iccsolutions.com) and we will provide you with the correct hash for that index.

## ***Certificate Authority Public Key 'E1'***

Length '70'

RID : A000009999

Index : E1

*Public Modulus is*

'99C5B70AA61B4F4C51B6F90B0E3BFB7A3EE0E7DB41BC466888B3EC8E9977C762407EF1D7  
9E0AFB2823100A020C3E8020593DB50E90DBEAC18B78D13F96BB2F57EEDDC30F256592417  
CDF739CA6804A10A29D2806E774BFA751F22CF3B65B38F37F91B4DAF8AEC9B803F7610E06  
AC9E6B'

*Public Exponent is*

'03'

Hash : 'F8707B9BEDF031E58A9F843631B90C90D80ED695'

## ***Certificate Authority Public Key 'E2'***

Length '70'

RID : A000009999

Index : E2

*Public Modulus is*

'BD232E348B118EB3F6446EF4DA6C3BAC9B2AE510C5AD107D38343255D21C4BDF4952A42E  
92C633B1CE4BFEC39AFB6DFE147ECBB91D681DAC15FB0E198E9A7E4636BDCA107BCDA33  
84FCB28B06AFEF90F099E7084511F3CC010D4343503E1E5A67264B4367DAA9A3949499272E  
9B5022F'

*Public Exponent is*

'03'

Hash : 'C1056ADCE9E6F76EA77C89CB832F5A4817907A1A'

**Certificate Authority Public Key 'E3'**

Length '70'

RID : A000009999

Index : E3

*Public Modulus is*

'BC01E12223E1A41E88BFFA801093C5F8CEC5CD05DBBDBB787CE87249E8808327C2D21899  
1F97A1131E8A25B0122ED11E709C533E8886A1259ADDFDCBB396604D24E505A2D0B5DD038  
4FB0002A7A1EB39BC8A11339C7A9433A948337761BE73BC497B8E58736DA4636538AD282D3  
CD3DB'

*Public Exponent is*

'010001'

Hash : '1B795CBB0830E2C5231704FA57424D1C4E50F3E4'

**Certificate Authority Public Key 'E4'**

Length '80'

RID : A000009999

Index : E4

*Public Modulus is*

'CBF2E40F0836C9A5E390A37BE3B809BDF5D740CB1DA38CFC05D5F8D6B7745B5E9A3FA696  
1E55FF20412108525E66B970F902F7FF4305DD832CD0763E3AA8B8173F84777100B1047BD1  
D744509312A0932ED25FED52A959430768CCD902FD8C8AD9123E6ADDB3F34B92E7924D729  
CB6473533AE2B2B55BF0E44964FDEA8440117'

*Public Exponent is*

'03'



Hash : 'AC8DA3E12324D719C1D5C9E6E8580157196EFEB9'

**Certificate Authority Public Key 'E5'**

Length '80'

RID : A000009999

Index : E5

*Public Modulus is*

'D4FDAE94DEDBECC6D20D38B01E91826DC6954338379917B2BB8A6B36B5D3B0C5EDA60B3  
37448BAFFEBCC3ABDBA869E8DADEC6C870110C42F5AAB90A18F4F867F72E3386FFC7E67E  
7FF94EBA079E531B3CF329517E81C5DD9B3DC65DB5F9043190BE0BE897E5FE48ADF5D3BF  
A0585E076E554F26EC69814797F15669F4A255C13'

*Public Exponent is*

'03'

Hash : 'ADA2349AFD118D55AF782D37B64651AF1CA61EE5'

**Certificate Authority Public Key 'E6'**

Length '80'

RID : A000009999

Index : E6

*Public Modulus is*

'EBF9FAECC3E5C315709694664775D3FBDA5A504D89344DD920C55696E891D9AB622598A9  
D6AB8FBF35E4599CAB7EB22F956992F8AB2E6535DECB6B576FA0675F97C23DD4C374A66E  
6AF419C9D204D0B9F93C08D789D63805660FBB629DF1B488CFA1D7A13E9B729437EEAFE71  
8EFA859348BA0D76812A99F31CD364F2A4FD42F'

*Public Exponent is*

'010001'

Hash : '8AA4F4648F0DC62AB6AED92554AD1A831BAFC9E4'

# Test Certificate Authority Public Keys For RID 'A000000004' - Mastercard profile for CT tests

## **Certificate Authority Public Key 'FE'**

Length '90'

RID : A000000004

Index : FE

*Public Modulus is*

'E76317965175A08BEE510F58830E87B262C70D529803245FA8B88E0C753562DE7AEB5A9E3E  
6C1A98E94D8DB7C31407DAC5D071E06B80B09E146F22DB85F1D72D1EA18D22600032C6DD  
40E3714D5ADA7DE9D7D01E88391F893156D6F4BF13E9063559DA0786DE9BDE6B1C9B0BB9  
68EDDE07145ABF877B931682CCB1FB800728724D04AF241E2827E0FA1F62591914FF25'

*Public Exponent is*

'010001'

Hash : '8535F14CBD6B4AE5028618FAB5AC1106549FD03C'

## **Certificate Authority Public Key 'FC'**

Length 'F8'

RID : A000000004

Index : FC

*Public Modulus is*

'B3296C91F4795BD97112606903407B6EFF3AB39246E91095E51D17867DA4ADE59A48BE2FE  
9B52710283D3D32260E2C7D247214C57D46AA6465E47E0A4B3FFAAD8A7F6A190755BCCFE3  
F3FB3989A9F6B1C9E1845BCCCAD6F20B1DAC6033600234E81DAC4153212B0F760C2309919  
2AA6C4C9083BEFFD9A79D2A27B08FECC8E5D437D6C68550A839B1294151DABA9D9CB2F16  
0F60F749289F500C8C7F334BD20EBAC4AB109CF3C182F1B781C7C097A7903530746C449B99  
E39E4DB6493DD2A02E37C62AE8BC9A7470ECCCF8DC06A18C33CD24B30D56F25D2755CE8  
2AA4DE4D2EAEC07750A03DB75EBD0D8EBC9F2A1D85A0D252EFF40329BE05'

*Public Exponent is*

'010001'

Hash : 'DB50B5B0D966300760B1E42125277BA833B65234'

**Certificate Authority Public Key 'FD'**

Length '90'

RID : A000000004

Index : FD

*Public Modulus is*

'C9485DBEB5E40415D1B397524F47685F306CFDC499D4E2E7D0CBAF222CFA8184BD111DAE  
EDC9CC6EC8540C3F7271EA9990119CC5C43180501D9F45252D6835053FAE35696AE8CD67A  
325647449CF5E594DA8F627209F7F03AE8D6DFC0DB3E79E28E415DF29A5B57D6814856CC3  
0A96DA5B8890363E507FCB2E283DA1EBB5F18E8E24102B7D0192BB8E35A4F7CD05A435'

*Public Exponent is*

'010001'

Hash : 'FC505E4A83FF29A3B1BD28DABF52599B2AE9CB14'

**Certificate Authority Public Key 'FB'**

Length '90'

RID : A000000004

Index : FB

*Public Modulus is*

'9B170603A489C7546C45DA57B8FFD1DB2061240F0E8C6D1F9ABDC6B265AA8911915C1A4E  
ABD8D0ED4755D1B902BA06FE5A645B786CD241295517D44EF1A7C25D75AFE0EB28066E4D  
69FEE7ABAFDD5EEB230F14E402C9840825FA77EAD12B5F1C5494701DE1897F65FE6BF106D  
47545EBF70CE7C158068C61F0773534DB742AB83C28038C1494F15905D0AD17CF1BD38D'

*Public Exponent is*

'010001'

Hash : 'FC787DB138F994A0C554CC6734EB3E48A55066CC'

**Certificate Authority Public Key 'FA'**

Length 'F8'

RID : A000000004

Index : FA

*Public Modulus is*

'A4203E0C7BEB27097B63C103C19FDCDA671AEA7F813065756F3B9B81810CBD4BC4DEC548  
FBF1F3CDAE51F847235CBF2C8BADD8ACA7C93BEA3D44E80ED6A7B70E29622619DB420AC  
CCE07E1DD4E6C354F359FBDC9C5B70813926F77D827E52B19DAF09BFAE5274438BB8F61D  
17753C9EC0A8EFA3B7E46F02692160D2653CDBCC71B7D48BD37968316EB444F6504B9421B  
7DD3035A2C117D8B1F76A8975440DA9563618102397B881CEF8ADA7689EDFACE32482A2DF  
FED656E7F951DB841DA78368C6293BFC1053A86A845BFA6578E4B69F100B42B558FDE1AEC  
EC6D250741BC783AA8A68A4261E7BB9246B10587A498D68DD955CE8B2B2433'

*Public Exponent is*

'010001'

Hash : '7F5ACBB96B589F74CB959ED1C35BDB965C3F4106'

**Certificate Authority Public Key 'FF'**

Length '90'

RID : A000000004

Index : FF

*Public Modulus is*

'F69DBB5E15983EAE3CCF31CF4E47098C2FC16F97A0C710F84777EFA99622D86502B138728  
AB12E3481A84D20E014AD2D634D2836F27F294924B895A87F91F81B8169D4DFDAD8D7CBD7  
41804CD61B467C7A9ACFECEB71188CAA73A907547699D45C9C7D2098AC2966266417F665A  
46BDD012C097DBD33D1D11AFF6EC8A9C0AD814A65B48262CA011636079A328C1AAEB7'

*Public Exponent is*

'010001'

Hash : '439EB23D8A71B99F879C1A1F1765252D840B9A74'

# Test Certificate Authority Public Keys For RID 'A000000065' - JCB profile for CT tests

## **Certificate Authority Public Key '02'**

Length '80'

RID : A000000065

Index : 02

*Public Modulus is*

'BB7F51983FD8707FD6227C23DEF5D5377A5A737CEF3C5252E578EFE136DF87B50473F9341  
F1640C8D258034E14C16993FCE6C6B8C3CEEB65FC8FBCD8EB77B3B05AC7C4D09E0FA1BA  
2EFE87D3184DB6718AE41A7CAD89B8DCE0FE80CEB523D5D647F9DB58A31D2E71AC677E6  
7FA6E75820736C9893761EE4ACD11F31DBDC349EF'

*Public Exponent is*

'010001'

Hash : 'B973E9F377B419C36AC9696ED95FFB25C8020687'

## **Certificate Authority Public Key '03'**

Length 'F8'

RID : A000000065

Index : 03

*Public Modulus is*

'C9E6C1F3C6949A8A42A91F8D0224132B2865E6D953A5B5A54CFFB0412439D54AEBA79E9B3  
99A6C104684DF3FB727C7F55984DB7A450E6AA917E110A7F2343A0024D2785D9EBE09F601  
D592362FDB237700B567BA14BBE2A6D3D23CF1270B3DD822B5496549BF884948F55A0D308  
348C4B723BAFB6A7F3975AC397CAD3C5D0FC2D178716F5E8E79E75BEB1C84FA202F80E68  
069A984E008706B30C212305456201540787925E86A8B28B129A11AF204B387CB6EE43DB53D  
15A46E13901BEBD5CECF4854251D9E9875B16E82AD1C5938A972842C8F1A42EBB5AE5336B  
04FF3DA8B8DFBE606FCA8B9084EE05BF67950BA89897CD089F924DBCD'

*Public Exponent is*

'03'

Hash : '7DC435DBDE093D1F0AD0BAE0FEA4DC12056413DC'

# Test Certificate Authority Public Keys For VISA RID 'A000000003'

## ***Certificate Authority Public Key '50'***

Length '80'

RID : A000000003

Index : 50

*Public Modulus is*

'D11197590057B84196C2F4D11A8F3C05408F422A35D702F90106EA5B019BB28AE607AA9CD  
EBCD0D81A38D48C7EBB0062D287369EC0C42124246AC30D80CD602AB7238D51084DED469  
8162C59D25EAC1E66255B4DB2352526EF0982C3B8AD3D1CCE85B01DB5788E75E09F44BE73  
61366DEF9D1E1317B05E5D0FF5290F88A0DB47'

*Public Exponent is*

'010001'

Hash : 'B769775668CACB5D22A647D1D993141EDAB7237B'

## ***Certificate Authority Public Key '51'***

Length '90'

RID : A000000003

Index : 51

*Public Modulus is*

'DB5FA29D1FDA8C1634B04DCCFF148ABEE63C772035C79851D3512107586E02A917F7C7E8  
85E7C4A7D529710A145334CE67DC412CB1597B77AA2543B98D19CF2CB80C522BDBEA0F1B  
113FA2C86216C8C610A2D58F29CF3355CEB1BD3EF410D1EDD1F7AE0F16897979DE28C6EF  
293E0A19282BD1D793F1331523FC71A228800468C01A3653D14C6B4851A5C029478E757F'

*Public Exponent is*

'03'

Hash : 'B9D248075A3F23B522FE45573E04374DC4995D71'

**Certificate Authority Public Key '53'**

Length 'F8'

RID : A000000003

Index : 53

*Public Modulus is*

BCD83721BE52CCCC4B6457321F22A7DC769F54EB8025913BE804D9EABBFA19B3D7C5D3C  
A658D768CAF57067EEC83C7E6E9F81D0586703ED9DDDADD20675D63424980B10EB364E81  
EB37DB40ED100344C928886FF4CCC37203EE6106D5B59D1AC102E2CD2D7AC17F4D96C398  
E5FD993ECB4FFDF79B17547FF9FA2AA8EEFD6CBDA124CBB17A0F8528146387135E226B00  
5A474B9062FF264D2FF8EFA36814AA2950065B1B04C0A1AE9B2F69D4A4AA979D6CE95FEE9  
485ED0A03AEE9BD953E81CFD1EF6E814DFD3C2CE37AEFA38C1F9877371E91D6A5EB59FD  
EDF75D3325FA3CA66CDFBA0E57146CC789818FF06BE5FCC50ABD362AE4B80996D'

*Public Exponent is*

'03'

Hash : 'AC213A2E0D2C0CA35AD0201323536D58097E4E57'

**Certificate Authority Public Key '96'**

Length '80'

RID : A000000003

Index : 96

*Public Modulus is*

B74586D19A207BE6627C5B0AAFBC44A2ECF5A2942D3A26CE19C4FFAE920521868922E89  
3E7838225A3947A2614796FB2C0628CE8C11E3825A56D3B1BBAEF783A5C6A81F36F8625395  
126FA983C5216D3166D48ACDE8A431212FF763A7F79D9EDB7FED76B485DE45BEB829A3D4  
730848A366D3324C3027032FF8D16A1E44D8D'

*Public Exponent is*

'03'

Hash : '7616E9AC8BE014AF88CA11A8FB17967B7394030E'

**Certificate Authority Public Key '57'**

Length '60'

RID : A000000003

Index : 57

*Public Modulus is*

942B7F2BA5EA307312B63DF77C5243618ACC2002BD7ECB74D821FE7BDC78BF28F49F74190  
AD9B23B9713B140FFEC1FB429D93F56BDC7ADE4AC075D75532C1E590B21874C7952F29B8  
C0F0C1CE3AEEDC8DA25343123E71DCF86C6998E15F756E3'

*Public Exponent is*

'010001'

Hash : '251A5F5DE61CF28B5C6E2B5807C0644A01D46FF5'

**Certificate Authority Public Key '58'**

Length 'C8'

RID : A000000003

Index : 58

*Public Modulus is*

99552C4A1ECD68A0260157FC4151B5992837445D3FC57365CA5692C87BE358CDCDF2C92FB  
6837522842A48EB11CDFFE2FD91770C7221E4AF6207C2DE4004C7DEE1B6276DC62D52A87  
D2CD01FBF2DC4065DB52824D2A2167A06D19E6A0F781071CDB2DD314CB94441D8DC0E936  
317B77BF06F5177F6C5ABA3A3BC6AA30209C97260B7A1AD3A192C9B8CD1D153570AFCC87  
C3CD681D13E997FE33B3963A0A1C79772ACF991033E1B8397AD0341500E48A24770BC4CBE  
19D2CCF419504FDBF0389BC2F2FDCD4D44E61F'

*Public Exponent is*

'010001'

Hash : '753ED0AA23E4CD5ABD69EAE7904B684A34A57C22'

**Certificate Authority Public Key '54'**

Length 'F8'



RID : A000000003

Index : 54

*Public Modulus is*

C6DDC0B7645F7F16286AB7E4116655F56DD0C944766040DC68664DD973BD3BFD4C525BCB  
B95272B6B3AD9BA8860303AD08D9E8CC344A4070F4CFB9EEAF29C8A3460850C264CDA39B  
BE3A7E7D08A69C31B5C8DD9F94DDBC9265758C0E7399ADCF4362CAEE458D414C52B49827  
4881B196Dacca7273F687F2A65FAEB809D4B2AC1D3D1EFB4F6490322318BD296D153B307A  
3283AB4E5BE6EBD910359A8565EB9C4360D24BAACA3DBFE393F3D6C830D603C6FC1E8340  
9DFCD80D3A33BA243813BBB4CEAF9CBAB6B74B00116F72AB278A88A011D70071E06CAB14  
0646438D986D48281624B85B3B2EBB9A6AB3BF2178FCC3011E7CAF24897AE7D'

*Public Exponent is*

'010001'

Hash : '06960618791A86D387301EDD4A3BAF2D34FEF1B4'

## **Test Certificate Authority Public Keys For RID 'A000000025' - AMEX profile for CT tests**

***Certificate Authority Public Key '60'***

Length '90'

RID : A000000025

Index : 60

*Public Modulus is*

'A8EE74EDEF3C0DCA5102FF9B5707975FF67B60D64B5E7322D48DE9D3BB6153F63512A091  
B606DD8FD5F6A14588324EF8827844C7FFC0BAB2334AE5207770078B69CDC3F2C666CF69E  
28E16E1816714C4DF313BEF539CC01DA9DD2D6F47DE4F247C500B561C099166AD4FC16DF  
12DFB684AC48D35CDD2C47A13A86A5A162306F64E33B092AB74EDA71A4091D96E3DAA47'

*Public Exponent is*

'010001'

Hash : '894B8DF19BDC691103C3B93979F5EE28C05888A7'

***Certificate Authority Public Key '61'***

Length 'F8'

RID : A000000025

Index : 61

*Public Modulus is*

'86C7254665E17CE6934DF7D082569F208D1CC1AD8E9FB2FE23E3D7467BE50B4F874F906AD  
F2280EC9D204F6D10C037A23CE5FD8283C9ED47D1C669ABDD7C1CB356C70BCDC44E5C8A  
E231555F7B786AC9C3155BCD51F28EFBC1B33CC87277049219B2C890952736C47134871116  
78911D9F42E08074CF524E65D721D727F054E6B5E85EC92B3EB59FFEE926DD6C314DF555C  
94AD487A99B67CB7C7BA5E46A5B813DDB918B8E3E0423F4302A58686D1263C0BACA9E8206  
8C493289E3E6936ECA5F9F77E06B0D6FBDA718818B835020098C671C5DD7E9B8E8E841D2D  
F32EE94A7F4748484CA44108AB241A5263BA1FF00D51360DDDC749D30A1'

*Public Exponent is*

'010001'

Hash : 'CCCF27C49C15B2A9410EC6089223A3A01EA8433E'

## Test Certificate Authority Public Keys For RID 'A000000152' - Discover profile for CT tests

***Certificate Authority Public Key 'D0'***

Length '90'

RID : A000000152

Index : D0

*Public Modulus is*

'D05C2A09D09C9031366EC092BCAC67D4B1B4F88B10005E1FC45C1B483AE7EB86FF0E884A  
19C0595A6C34F06386D776A21D620FC9F9C498ADCA00E66D129BCDD4789837B96DCC7F09  
DA94CCAC5AC7CFC07F4600DF78E493DC1957DEBA3F4838A4B8BD4CEFE4E4C6119085E5B  
B21077341C568A21D65D049D666807C39C401CDFEE7F7F99B8F9CB34A8841EA62E83E8D63'

*Public Exponent is*

'010001'

Hash : 'DE1BB8A37CDDDBCEAAB043AAEF81634120349726D'

***Certificate Authority Public Key 'D1'***

Length 'F8'

RID : A000000152

Index : D1

*Public Modulus is*

'A71AF977C1079304D6DFF3F665AB6DB3FBDF A1B170287AC6D7BC0AFCB7A202A4C815E1F  
C2E34F75A052564EE2148A39CD6B0F39CFAEF95F0294A86C3198E349FF82EECE633D50E58  
60A15082B4B342A90928024057DD51A2401D781B67AE7598D5D1FF26A441970A19A3A58011  
CA19284279A85567D3119264806CAF761122A71FC0492AC8D8D42B036C394FC494E03B4360  
0D7E02CB5267755ACE64437CFA7B475AD40DDC93B8C9BCAD63801FC492FD251640E41FD1  
3F6E231F56F97283447AB44CBE11910DB3C75243784AA9BDF57539C31B51C9F35BF8BC2495  
762881255478264B792BBDCA6498777AE9120ED935BB3E8BEA3EAB13D9'

*Public Exponent is*

'010001'

Hash : 'FFDA858CB2AF08B79D750CC97FA6EFE2EF228DDA'

## **Test Certificate Authority Public Keys For RID 'A000000333' - CUP profile for CT tests**

***Certificate Authority Public Key 'C0'***

Length '90'

RID : A000000333

Index : C0

*Public Modulus is*

'C7CDB6F2A3FE80A8834CDDDD326E1082AA2288F47C464D57B34718193431711A441191480  
55044CFE3313708BED0C98E1C589B0F53CF6D7E829FCD906D21A90FD4CB6BAF13110C468  
5107C27E00981DB29DC0AC186E6D701577F23865626244E1F9B2CD1DDFCB9E899B41F5084  
D8CCC178A7C3F4546CF93187106FAB055A7AC67DF62E778CB88823BA58CF7546C2B09F'

*Public Exponent is*

'010001'

Hash : '8B094D260BDF8BFC8B9A88B0C177A43FE2FAE765'

**Certificate Authority Public Key 'C1'**

Length 'F8'

RID : A000000333

Index : C1

*Public Modulus is*

'92F083CBE46F8DCC0C04E498BA9952BA9D4C09C80DD277E579F07E45772846FA43DD3AB3  
1CC6B08DD18695715949FB108E53A071D393A7FDDBF9C5FB0B0507138797317480FC48D633  
ED38B401A451443AD7F15FACDA45A62ABE24FF6343ADD0909EA8389348E54E26F842880D1  
A69F9214368BA30C18DE5C5E0CB9253B5ABC55FB6EF0A738D927494A30BBF82E340285363  
B6FAA15673829DBB210E710DA58EE9E578E7CE55DC812AB7D6DCCE0E3B1AE179D664F335  
6EB951E3C91A1CBBF6A7CA8D0C7EC9C6AF7A4941C5051099B9784E56C9162067B8C3B15C  
5FA4480A645CD2526A69C80BA8EF361BE2AA9417DEFCE35B62B0C9CF097D'

*Public Exponent is*

'010001'

Hash : 'B6372DB9919F8C6C9C88E83D3C600A4AD8ADC7A9'