INTERNAL USE

Keymaster For Android O

KEYMASTER 3.0 NOTE

What's New in Keymaster 3.0

- Keymaster HIDL service
  - Android O has system partition (AOSP) and vendor partition (OEM)
    - Socket connection between system partition and vendor partition is forbidden
    - HIDL is the only method for connection between system partition and vendor partition

What's New in Keymaster 3.0

- Root of Trust (RoT) binding
  - Guarantee system image is not altered after verified boot
    - Both verified boot and Android system provide keymaster the information of OS version and OS patch level
    - Keymaster refuses to operate if the information does not match
  - RoT information is also bound in key blob
    - Keymaster returns KM_ERROR_KEY_REQUIRES_UPGRADE if a key blob contains old OS version or OS patch level
    - Keymaster provides upgrade_key() interface to upgrade the key blob

What's New in Keymaster 3.0

- Key attestation support
  - How to make sure that a key is really generated by the HW keymaster?
    - A certificate of the key is signed by the HW keymaster
    - The certificate can be verified via Google PKI
  - Customer needs to request a signing key from Google and install the key for the HW keymaster
    - Attestation key provisioning in kb partition

OTA Issue

- Limitation
  - Keymaster 1.0 cannot be upgraded to keymaster 3.0
    - Attestation key provision is only in factory stage
    - RoT information is not bound in key blob
  - Policy
    - Devices from Android N to Android O must use keymaster 1.0
    - New devices with Android O will use keymaster 3.0

The Problem

- How to make sure that a key is really generated by the HW keymaster?
  - A certificate of the key is signed by the HW keymaster
- We need to install an attestation key to the HW keymaster
  - For the purpose of signing certificate

Keybox.xml

- Obtain from Google
  - A keybox.xml can include many attestation keys
  - At least 100000 devices share one attestation key
- PEM format
  - The attestation key contains one ECDSA key with cert-chain and one RSA key with cert-chain

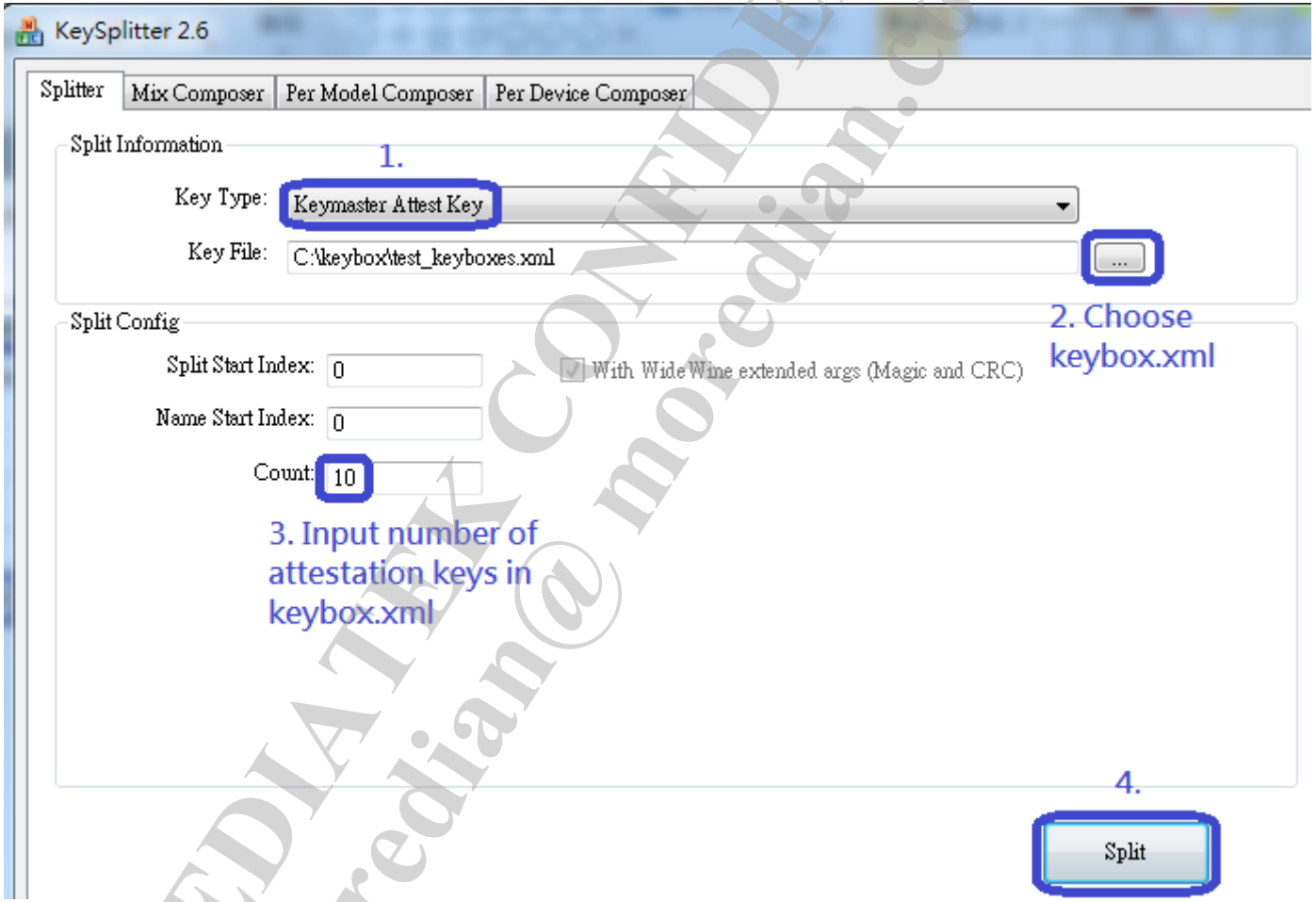
Sample

- - <AndroidAttestation>
- <NumberOfKeyboxes>10</NumberOfKeyboxes>
- - <Keybox DeviceID="dev1">
- - <Key algorithm="ecdsa">
- <PrivateKey format="pem">-----BEGIN EC PRIVATE KEY----- MHcCAQEEIJsBK6DXJKTH8ObUHYwoAy5Cdk6I6y+WT9DnWDKNaSy0oAoGCCqGSM49
AwEHoUQDQgAEi7SBOsnFExykOVUfupIzNEFrT47dE0aKKQ6weAi4v9HoZClffWcY SKvqBxtdmRxQuN/NVLq4OupPGv09+Cm4fA== -----END EC PRIVATE KEY-----</PrivateKey>
- - <CertificateChain>
- <NumberOfCertificates>3</NumberOfCertificates>
- <Certificate format="pem">-----BEGIN CERTIFICATE----- MIICLDCCAbKgAwIBAgIKAZQwVVNkZ0RkKTAKBggqhkjOPQQDAjAbMRkwFwYDVQQF
ExA1MzVkYTAwMzIxY2FiZmY2MB4XDTE2MDYwMzE1NTYzNloXDTI2MDYwMTE1NTYz NlowGzEZMBcGA1UEBRMQMTkwMmFiZTM3ZjNmZTA1YjBZMBMGByqGSM49AgEGCCqG
SM49AwEHA0IABIu0gTrJxRMcpDlVH7qSMzRBa0+O3RNGiikOsHgIuL/R6GQpX31n GEir6gcbXZkcULjfzVS6uDrqTxr9PfgpuHyjgd0wgdowHQYDVR0OBBYEFAb/Ik+m
Dkk9O6CzEzpOYx1AUj8wMB8GA1UdIwQYMBaAFJV0LzicBzbW6UbsAH5EchNclUAB MAwGA1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgeAMCQGA1UdHgQdMBugGTAXghVp
bnZhbGlkO2VtYWlsOmludmFsaWQwVAYDVR0fBE0wSzBJoEegRYZDaHR0cHM6Ly9h bmRyb2lkLmdvb2dsZWFwaXMuY29tL2F0dGVzdGF0aW9uL2NybC8wMTk0MzA1NTUz
NjQ2NzQ0NjQyOTAKBggqhkjOPQQDAgNoADBlAjAdBYVnzLh0rNM03gMR7m4Gr09q n7Xn86o8jJQbcF1kuAVDGa1Kc1GkffKxqsagpLYCMQD8ogDHiZPKVeDXGg82sowu
sfoRMI34FI+DKNmBC5A5EPRzSUqi1Brb/FGSsAYT5jc= -----END CERTIFICATE-----</Certificate>
- <Certificate format="pem">-----BEGIN CERTIFICATE----- MIIDwzCCAaugAwIBAgIKEFeBFwEJECgCDDANBgkqhkiG9w0BAQsFADAbMRkwFwYD
VQQFExAwMGZjMzc0MzIzNWUwMDM3MB4XDTE2MDYwMzE1NTYyOFoXDTI2MDYwMTE1 NTYyOFowGzEZMBcGA1UEBRMQNTM1ZGEwMDMyMWNhYmZmNjB2MBAGByqGSM49AgEG
BSuBBAAiA2IABObfzVifA4f9XYfGjE5WX4g5OnP5E0FjkYDMLmQTj3vFfBP7mhDb 0PN3X1jh1DknXdbtV/RfLID/oVmkapp7wxrJvo3tKi2gNeB34cx6OQ32rJjCNkky
tszsrZzrZAebEaOBtjCBszAdBgNVHQ4EFgQUlXQvOJwHNtbpRuwAfkRyE1yVQAEw HwYDVR0jBBgwFoAUEGaiIRAGzOq05rxthbjJV1xcMn0wDwYDVR0TAQH/BAUwAwEB
/zAOBgNVHQ8BAf8EBAMCAYYwUAYDVR0fBEkwRzBFoEOgQYY/aHR0cHM6Ly9hbmRy b2lkLmdvb2dsZWFwaXMuY29tL2F0dGVzdGF0aW9uL2NybC8xMzg5QjE2NUUzOTI4
RTY4MA0GCSqGSIb3DQEBCwUAA4ICAQAmZ72caC9Rov1+nqBozmNFt9kk9tLBZh8d LIsG0R/tmFcX2nIi3PZhBJJb9fdzFSNBuuxDKqAlhrdNkXyVBIexMWToP2Z2gr/S
BG8+J/7CIrGSm1rzX3HLEKiNUSn234ZJUu0gDmXR6QkRxMLqcsbP9KggbKcU86Vw u6+pe+RI48hK5d/KJO3obGoDHDXP6OLSL97Lb1S9uepu0R2s4SHsPou+/QhaSb4F
93eILddxBOnqvhd3lfK7742LzRZGtQn6ZNKWi/ryASIbxS6GlVPX5zfDKzNqTg0w 52sJJXy+tAd5cfVSXmWAHg3KplnEyjSUseD1cpgIATc8uqh9n/qfs11B8HxDK8l4
x7g8m2vRnRc+mhIOyx/LsOL6Jf2+ARoZsM6Q88eGNx+cqP/lVXQXx2SRin2tTm0k NINpdnZriTODIM/qUlmnDKiMUpOubABJk6XuIwzJ8TJWD8VHnqQOovdkG+uzLgIi
zfQLh/ECsUsIWcSK6/ehPsYP3ENoSZaT0BC3SaHeJignzto2Hg/KbAr2/66xd8rB athadEI6ifAumaYqrqmMHVusCZu+Rlabk4Shz8S21Ar+E6stW17b9hlBVlsufcDu
YJU/m8FamIPQc1KORQOBeDXknjxNHZU+5b4qcNqTXgCMYA6PPti6saDRPYWi+878 hl6/wZNnpg== -----END CERTIFICATE-----</Certificate>
- <Certificate format="pem">-----BEGIN CERTIFICATE----- MIIFXzCCA0egAwIBAgIIE4mxZeOSjmgwDQYJKoZIhvcNAQELBQAwGzEZMBcGA1UE
BRMQMDBmYzM3NDMyMzVlMDAzNzAeFw0xNjA2MDMxNTUyNDhaFw0yNjA2MDExNTUy NDhaMBsxGTAXBgNVBAUTEDAwZmMzNzQzMjM1ZTAwMzcwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDToBSa9b3XjReBGX9dOLPBvoz7oYA4Gym4JrmMoe4m n7GeXq/0+2ys/aoFIaQS+I//3d9VsSGiDqR3bo+dgl4rgdoNTNAnr09CDV2SFijv
Yfs1F/1aGq8ltaIJEvMJjZJpdkHNc2PEic+ZZrDPg3fPmXOMbHRispahYZCof3sG /uPXqm5P9yt5umCPaEJ/34CtXRMAMj0S4ffAAHJRKmzeLlpj4UgfEuxXasw1WLXT
0P1BYkCoLDdZWgqYS5TFl/xlES9BfH5cfg+2rNlA/GpsRI8VYEM+c9zusK0Sr+YE OO1HWjHuJgHbHVAChxO2zdzs9njjojEc9D5v7Zk3jwTzO9LahCXBjkrJew0yF4oE
Z8/7PVFmPqlk5DzJsFmrCAPdacSQo1fFQ22SHq1lqM7OYE/+F+JaptGnfr4q1lZI jiUKVe0Dh3JbtanlS44bdQaj1TK6S1ETlZRYXE3hvCFmfeD1aChqIZuAqy2LhCrU
YXuGYRl99tEefixa8gJrZHsVStB6oy0E+0/+a7v9/hF9GM4Mldg9mdKvpjoCXmJj B5L0EVyWvxZxlsIWQV+tQPc0V6n3wFRfb7+a+lkDnKaWftIZN7mr64Xh1YBnRzQG
ogp9kQsI2FO/MBSi6iTW4Te4YK1p/UpSYaZlnZRq8rX1Mr9V449mtcVA5KQT3rjE IQIDAQABo4GmMIGjMB0GA1UdDgQWBBQQZqIhEAbM6rTmvG2FuMlXXFwyfTAfBgNV
HSMEGDAWgBQQZqIhEAbM6rTmvG2FuMlXXFwyfTAPBgNVHRMBAf8EBTADAQH/MA4G A1UdDwEB/wQEAwIBhjBABgNVHR8EOTA3MDWgM6Axhi9odHRwczovL2FuZHJvaWQu
Z29vZ2xlYXBpcy5jb20vYXR0ZXN0YXRpb24vY3JsLzANBgkqhkiG9w0BAQsFAAOC AgEAUN0yJGzqHhVfbpNctazlI36WUbzadR9+LJHe+nlxjkUH4sigqdxA5TbwVmPUu
/mEmUizyVL6TLWhwINxu+uM0FGkdfYCTpcfJliIlNcXWcXEMqIhl5MBdNmNIOhEH TVmmcGgrZTmwMIViLZzy+bG9qaCiiIG5xPlZ+30XLth/M+/ZkKjJ4zUY6L8Ir2M6
ttxGPvTFcr6ybwOFWDUOmfDyie0l2CwU/rcJFitrAWBZ7dq4I44Td+SRzSndjE/m /EZa7tW6h5LB2Y3AzOOuZsqlA/TbSnE8g80Rdvj78zXLKCghEMZFYe+cVJ7aDKRT
ebUcz0dZLItwMDVA8I2QoBvERz3eGBD1qMW6feAZD/z29nTaQyLo9EJyxhHOMQ01 yBBPlIC78DH7vnaENb6iheVjtRf82LydSTIdzYZgOHch4rOcxmUDj7PbyzjVokwa
dc9h01bjJXmbKFGokHAXBwXMIZphH52fw5xeGnIsxPdQiybw4OOtsxjNm70Xo+MY h/R6f7Gd+HFK8CIfIw0y6B45ubXBAu0nD3mctcSvTwqjE4A0yEfrlsxeiioZsnLC
JRTBVS8GyLQFZWNzvVDoTrN5mE5d4TiJoxkxfMN15vjLjlrmqCh3C541ztNT07DV /AI0IK0ObR0lNniV94ZfUq/ztEjWX+nuGYrSSCEU2cNr4GU= -----END CERTIFICATE-----</Certificate>
- </CertificateChain>
- </Key>

KeySplitter Tool

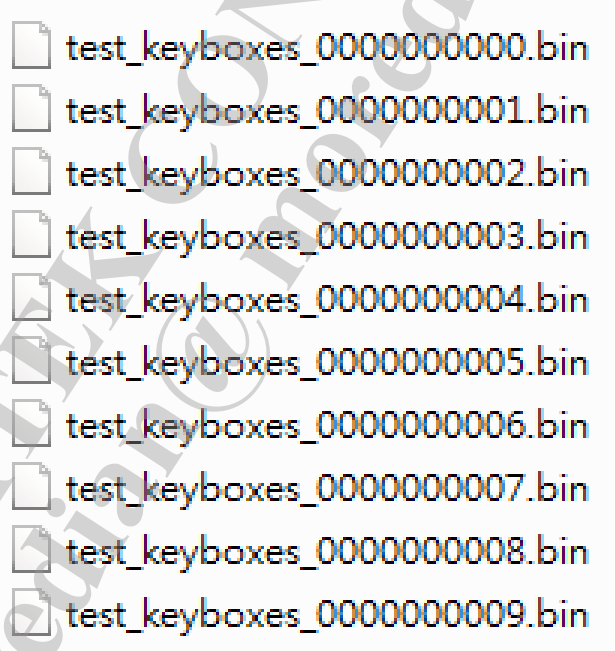
- Splitter
  - Convert PEM to DER format
  - One file contains one attestation key
- Mix Composer
  - Keep the attestation key safe in factory
  - Customer has to customize the encryption keys

Splitter



Splitter Result

- keybox\splitter\keymaster_attestation



Mix Composer

KeySplitter 2.6

Splitter | Mix Composer | Per Model Composer | Per Device Composer

Key Block File Config

Name: kb

Start Idx: 0

Count: 1

Custom Key: C:\keybox\Kkb

Encrypt Key: C:\keybox\Kkb_pri

1. Choose Kkb

2. Choose Kkb_pri

HDCP 1.X TX Key
First Key File:

HDCP 1.X RX Key
First Key File:

HDCP 2.X TX Key
Key File:

HDCP 2.X RX Key
First Key File:

WideVine Key
First Key File:

Playready Model Cert
Cert File:

Playready Model Key
Key File:

Marlin Key
Marlin File:

Keymaster Attest Key
First Key File: C:\keybox\splitter\keymaster_attestat

3. Choose key in splitter\keymaster_attestation

4.

Compose

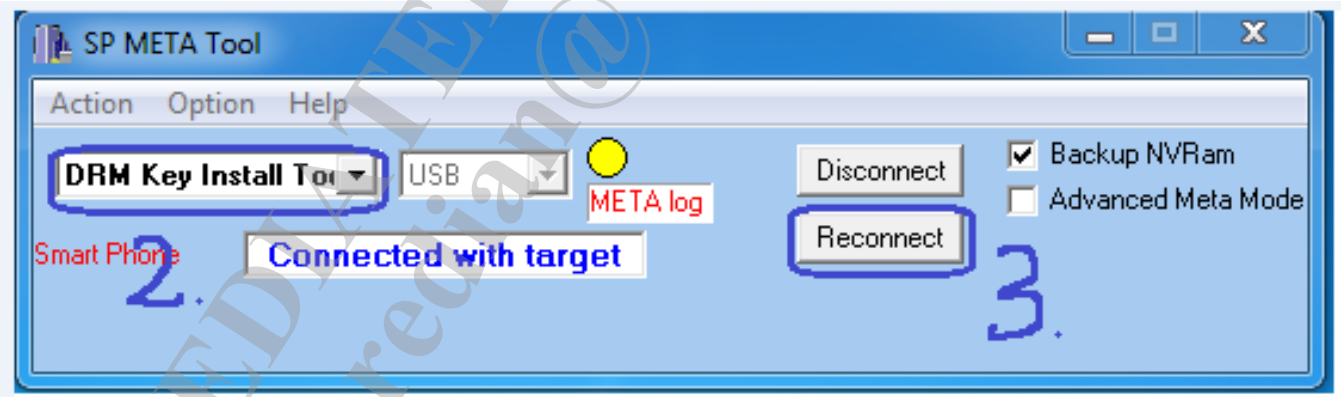
Mix Composer Result

- keybox\composer

kb_0000000000.bin

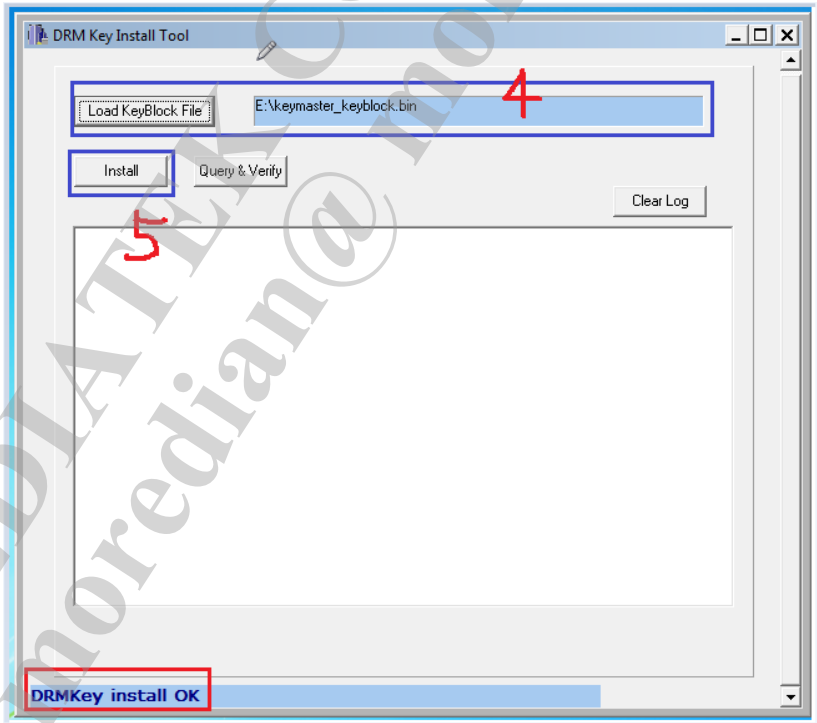
SP Meta Tool

- Install attestation key to device
  1. Launch “SP Meta Tool”
  2. Choose “DRM Key Install Tool”
  3. Reconnect device



SP Meta Tool

- After connecting to device
  4. Load KeyBlock File
  5. Install attestation key
  6. Disconnect device

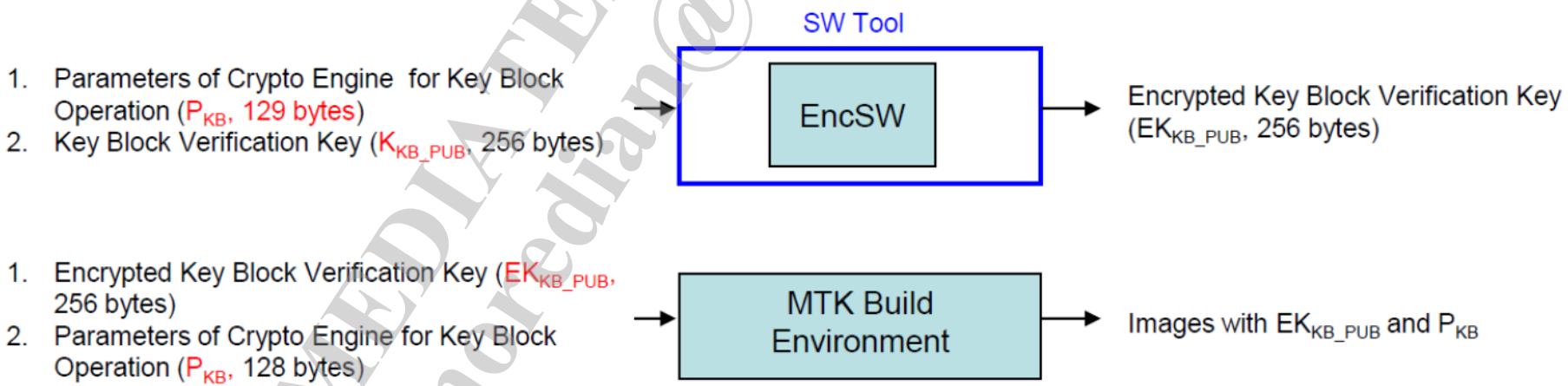


Appendix

HOW TO CUSTOMIZE ENCRYPTION KEY

Customize Encryption Key

1. Prepare keys P_{KB}, K_{KB}, and (K_{KB_PRI}, K_{KB_PUB})
2. Use EncSW to generate EK_{KB_PUB}
3. Put (P_{KB}, EK_{KB_PUB}) in source code and re-build image



Parameter P_{KB} (129 bytes)

- openssl rand -hex 128

Step1. Use "**openssl rand –hex 128**" command generate the 128 Bytes random number

```
jyfu@pc0911061810: ~
jyfu@pc0911061810:~$
jyfu@pc0911061810:~$ openssl rand -hex 128
9c28c76c75765f841efc6aec8711efa96c7f469141de2a93c2b7cf2100f1714afb609a2b
4a89e0ec997e1cbe2a61b068292d7ab31e9842b524fbb9fccfbe2c274aa5abc7823029809
24c1bb68e6f4b884ccb52f4d6f121d193acc0bf222492655c571cd3b3763abc5f361c0b8
847c9a10ff98e06c
```

Step 2. You need to add one byte "00" at first. Then copy the random number to text file and save it. The total length is 129 bytes.

```
File  Edit  Format  View  Help
009c28c76c75765f841efc6aec8711ef
469141de2a93c2b7cf2100f1714afb60
54a89e0ec997e1cbe2a61b068292d7ab
9fccfbe2c274aa5abc7823029809c
332b0324c1bb68e6f4b884ccb52f4d6f
92655c571cd3b3763abc5f361c0b872d
```

AES-128 IV-Key K_{KB} (32 bytes)

- openssl rand -hex 32

Step1. Use "**openssl rand –hex 32**" command generate the 32 Bytes random number

```
jyfu@pc0911061810: ~
jyfu@pc0911061810:~$ openssl rand -hex 32
72f162dc7c7e92011e8a43a02778c26912575105f9031a5c9dfedece6d24c545
jyfu@pc0911061810:~$
```

```
File  Edit  Format  View  Help
72f162dc7c7e92011e8a43a02778c26912575
```

Step 2. Copy random number to file and save it.

RSA-2048 Key Pair (K_{KB_PRI}, K_{KB_PUB})

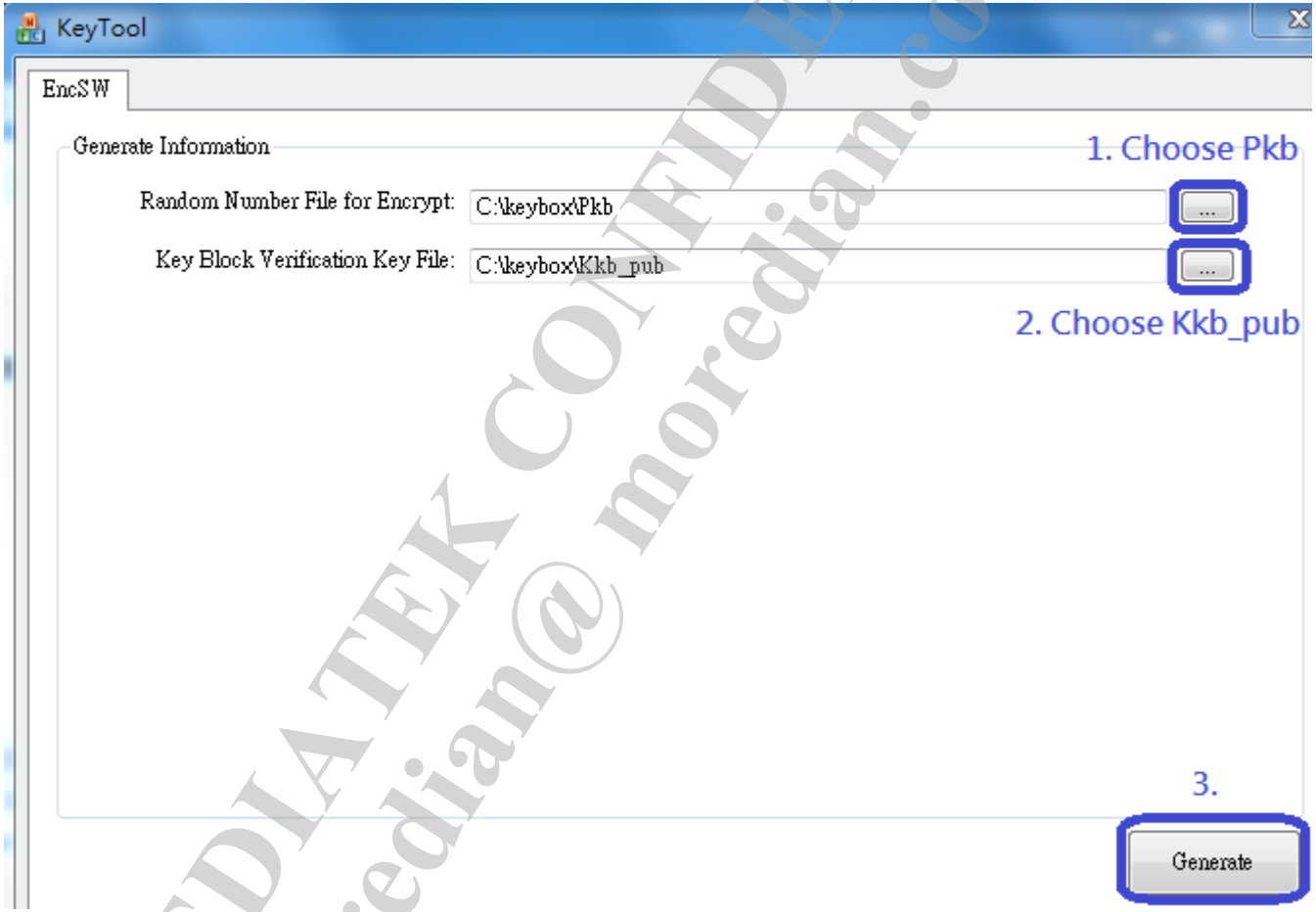
- K_{KB_PRI}
  - openssl genrsa -out Kkb_pri.pem 2048
  - openssl rsa -inform PEM -in Kkb_pri.pem -outform DER -out Kkb_pri
- K_{KB_PUB}
  - openssl rsa -text -in Kkb_pri.pem -pubout
  - Remove the first byte “00:” and save as file Kkb_pub

RSA-2048 Key Pair (K_{KB_PRI}, K_{KB_PUB})

```
jyfu@pc0911061810: ~
jyfu@pc0911061810:~$ openssl rsa -text -in Kkb_pri.pem -pubout
Private-Key: (2048 bit)
modulus:
    00:bb:97:c8:84:85:8f:a4:5e:3e:2c:d8:24:58:28:
    fd:22:9c:8b:54:f0:3a:ae:cc:e3:02:b6:ea:49:1f:
    6e:14:8a:cd:0e:a4:43:ff:91:a9:13:8b:72:48:06:
    7c:3c:8c:90:91:f3:2a:91:3d:09:71:4f:5b:dc:37:
    16:53:bd:8c:e5:ad:21:63:c5:28:5e:fe:06:36:88:
    16:d9:bc:88:f3:c1:89:01:c4:61:55:0d:65:aa:9e:
    31:30:83:d2:25:77:21:7d:e2:7d:50:ad:e7:3f:51:
    3e:92:df:f0:56:73:96:34:4e:9f:25:2f:86:f4:a2:
    fe:3e:0b:30:b1:9c:04:46:e7:c3:72:61:cc:1b:5a:
    57:1b:86:c0:e2:96:63:bc:bb:46:80:15:91:f5:50:
    62:1a:7f:0e:3b:94:89:fc:2f:5e:e2:2c:42:69:a1:
    8b:74:df:bc:3f:78:92:e2:3a:4b:43:fd:5c:a9:ee:
    d5:99:6b:fb:4b:dc:39:e5:47:18:da:34:fe:a1:fd:
    c0:e1:c2:b1:f6:19:3e:70:b0:55:22:03:de:f7:09:
    eb:b9:fa:06:4b:a4:3a:ef:de:53:50:85:69:c0:71:
    d6:c4:3a:3e:72:21:8a:0a:d8:21:21:9b:a6:55:5c:
    70:81:6f:d3:30:e4:de:f4:25:34:92:5f:f4:89:3f:
    3f:51
publicExponent: 65537 (0x10001)
privateExponent:
    00:aa:74:aa:f1:2f:e3:6b:b9:6e:c9:
```

```
File Edit Format View Help
bb:97:c8:84:85:8f:a4:5e:3e:2c:d8:24:58:28:
fd:22:9c:8b:54:f0:3a:ae:cc:e3:02:b6:ea:49:1f:
6e:14:8a:cd:0e:a4:43:ff:91:a9:13:8b:72:48:06:
7c:3c:8c:90:91:f3:2a:91:3d:09:71:4f:5b:dc:37:
16:53:bd:8c:e5:ad:21:63:c5:28:5e:fe:06:36:88:
16:d9:bc:88:f3:c1:89:01:c4:61:55:0d:65:aa:9e:
31:30:83:d2:25:77:21:7d:e2:7d:50:ad:e7:3f:51:
3e:92:df:f0:56:73:96:34:4e:9f:25:2f:86:f4:a2:
fe:3e:0b:30:b1:9c:04:46:e7:c3:72:61:cc:1b:5a:
57:1b:86:c0:e2:96:63:bc:bb:46:80:15:91:f5:50:
62:1a:7f:0e:3b:94:89:fc:2f:5e:e2:2c:42:69:a1:
8b:74:df:bc:3f:78:92:e2:3a:4b:43:fd:5c:a9:ee:
d5:99:6b:fb:4b:dc:39:e5:47:18:da:34:fe:a1:fd:
c0:e1:c2:b1:f6:19:3e:70:b0:55:22:03:de:f7:09:
eb:b9:fa:06:4b:a4:3a:ef:de:53:50:85:69:c0:71:
d6:c4:3a:3e:72:21:8a:0a:d8:21:21:9b:a6:55:5c:
70:81:6f:d3:30:e4:de:f4:25:34:92:5f:f4:89:3f:
3f:51
```

Use EncSW to generate EK_{KB_PUB}



EncSW Result

- keybox\encsw\array.c
  - unsigned char Ekkb_pub[]

```
unsigned char Ekkb_pub[] =
 {
    0x54, 0xCB, 0xCD, 0xB3, 0xFF, 0xCD, 0xCC, 0xDD, 0xA3, 0xFF, 0x5D, 0x30, 0x95, 0x03, 0x2D, 0x2A,
    0x2A, 0x12, 0xE6, 0x90, 0x0B, 0x3F, 0xF7, 0x85, 0xE5, 0xB3, 0xDD, 0x8E, 0x4B, 0x27, 0x9D, 0x58,
    0xC8, 0x24, 0x7A, 0xB0, 0x83, 0x8B, 0xB1, 0xD4, 0xA4, 0x92, 0x17, 0x0E, 0xF2, 0xCF, 0x19, 0x9A,
    0xAB, 0xCE, 0xFB, 0x68, 0xCB, 0x86, 0x94, 0x6E, 0x16, 0x8E, 0x3D, 0xCC, 0xF8, 0x0C, 0xA6, 0x30,
    0x1C, 0x47, 0xA6, 0xB6, 0x50, 0x2F, 0x68, 0x94, 0x23, 0x0C, 0x62, 0xAF, 0xE1, 0x44, 0xA4, 0x27,
    0xD8, 0x79, 0x05, 0x68, 0x51, 0x89, 0x04, 0x49, 0x61, 0x93, 0x7A, 0xEF, 0xB5, 0xB9, 0x17, 0x72,
    0x28, 0x87, 0xBA, 0x94, 0x4A, 0xB8, 0xF1, 0x46, 0xCF, 0xE7, 0x53, 0x0A, 0x02, 0x5A, 0xEE, 0x59,
    0x47, 0xBE, 0xC2, 0x41, 0x98, 0xD9, 0x5B, 0x17, 0xAF, 0x10, 0x0B, 0xE0, 0x92, 0xBA, 0x65, 0x30,
    0x63, 0x76, 0x94, 0x2A, 0x26, 0x7D, 0x3F, 0x94, 0x2E, 0x9F, 0x06, 0xB8, 0xD3, 0xB0, 0x76, 0xE9,
    0xBD, 0xBA, 0x07, 0x6E, 0xE1, 0x3D, 0x1F, 0xC6, 0xDB, 0x7F, 0x34, 0xC1, 0xB4, 0xED, 0x8B, 0x00,
    0x36, 0xAE, 0x1E, 0xBB, 0x65, 0x81, 0x38, 0x94, 0x77, 0xE2, 0x4E, 0x5C, 0xC1, 0x9F, 0x93, 0x2D,
    0x29, 0xA3, 0x30, 0x29, 0xF7, 0xEC, 0xFC, 0xCC, 0x87, 0x3F, 0xFA, 0x09, 0xAD, 0x1E, 0xE5, 0xAF,
    0x4E, 0xCF, 0x0E, 0x44, 0x8C, 0xE3, 0xBF, 0x8D, 0x5B, 0xEB, 0xD6, 0xA0, 0xEA, 0xC6, 0xBF, 0xB1,
    0x56, 0xD5, 0xC9, 0xE6, 0xB8, 0xE1, 0xB9, 0x94, 0x85, 0xAD, 0x38, 0x38, 0xDD, 0xE2, 0x57, 0xCC,
    0xFE, 0xED, 0xF0, 0x2A, 0x10, 0xB6, 0x8E, 0x3C, 0xA2, 0x4D, 0x97, 0x60, 0x3E, 0xEC, 0x92, 0xE2,
    0xC1, 0x72, 0xB6, 0x38, 0xE2, 0xC0, 0xA8, 0xCA, 0xD6, 0xEB, 0x0C, 0x35, 0xE9, 0x3E, 0x8D, 0x91,
 };
```

EncSW Result

- keybox\encsw\array.c
  - unsigned char InputPkb[]

```
unsigned char InputPkb[] =
{
    0x00,
    0x05, 0x14, 0x24, 0x14, 0x2F, 0xE1, 0xFC, 0x61, 0xB1, 0x0B, 0x97, 0xAF, 0x5C, 0x66, 0xB0, 0xF6,
    0x15, 0x26, 0xF6, 0x1C, 0x96, 0xC8, 0xBA, 0x96, 0x77, 0xD5, 0x4E, 0xFB, 0xA4, 0x91, 0xFD, 0xFB,
    0x16, 0x33, 0xED, 0x6E, 0xCC, 0x41, 0x0F, 0xCF, 0xC2, 0x94, 0xC2, 0x64, 0x1C, 0xFA, 0x12, 0x66,
    0x04, 0xE3, 0x4C, 0xF0, 0xB4, 0x5F, 0x15, 0x4B, 0xDB, 0xF4, 0x29, 0x1F, 0x98, 0xD3, 0xF5, 0x4E,
    0xA8, 0xD2, 0xA1, 0x0E, 0x8B, 0x59, 0xBF, 0x17, 0xDE, 0xB7, 0xA7, 0x50, 0x02, 0x2F, 0x14, 0x9C,
    0x7A, 0xE5, 0x24, 0x6D, 0x0E, 0x9F, 0xDE, 0x45, 0x4D, 0x6A, 0x75, 0x06, 0xB3, 0xDA, 0x88, 0x86,
    0x8D, 0xA6, 0x11, 0x43, 0xA8, 0x17, 0xA9, 0x6F, 0x70, 0x27, 0x01, 0xDA, 0xFA, 0xAF, 0xF6, 0xA8,
    0x47, 0xEC, 0xEF, 0x29, 0x66, 0x4E, 0xA8, 0x7C, 0x99, 0xFA, 0x40, 0xB8, 0xD4, 0x8A, 0x2C, 0xB1,
};
```

Put (P_{KB}, EK_{KB_PUB}) in Source Code

- Update Ekkb_pub[] and InputPkb[] in key.c
  - MTEE
    - vendor/mediatek/proprietary/custom/${project}/drm

MEDIATEK

everyday genius