BootCamp Quick Reference

Disclaimer:

The Bootcamp source code is forked from Infineon GitHub, frozen and modified for training purposes. Hence, it is neither updated regularly nor qualify for production. Please refer to official Infineon GitHub https://github.com/Infineon/arduino-optiga-trust-x for the updated and latest release.

BootCamp Github:

https://github.com/gilatoes/arduino-optiga-trust-x

BootCamp Mission:

https://github.com/gilatoes/arduino-optiga-trust-x/blob/master/Missions/MissionTasks.md

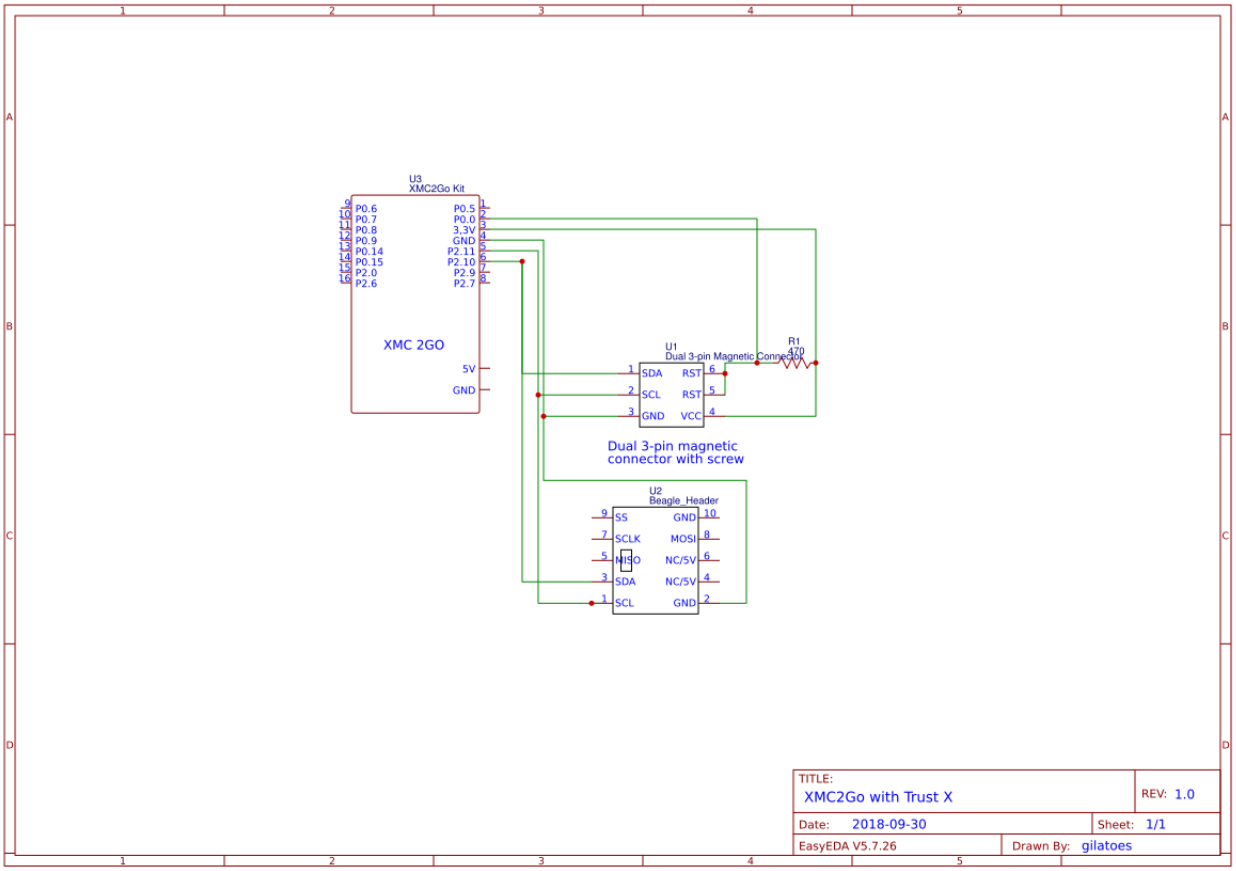
Additional Boards Manager URL:

https://github.com/Infineon/Assets/releases/download/current/package_infineon_index.json

Arduino Trust X Library Path:

C:\Users\xxxx\Documents\Arduino\libraries\arduino-optiga-trust-x\

Exerciser Schematic:



Source: https://easyeda.com/gilatoes/mission-1-xmc2go

Trust X Quiz:

https://kahoot.it/

Focus algorithms in BootCamp: ECC and SHA256. Ignore RSA.

Commonly used OpenSSL commands for this BootCamp:

Check OpenSSL version

```
openssl version
```

Generate ECC Private key

```
openssl ecparam -name prime256v1 -genkey -noout -out <private.key.pem>
openssl ecparam -name secp384r1 -genkey -noout -out <private.key.pem>
```

Generate ECC Public Key

```
openssl ec -in <private.key.pem> -outform PEM -pubout -out <public.key.pem>
```

Display certificate

```
openssl x509 –noout –text –in <cert.pem>
```

Verify certificate chain

```
openssl verify -CAfile <RootCA_cert> -untrusted <IntermediateCA_cert>
<EndDevice_cert>
```

Hash a file message

```
openssl dgst -sha256 <message_file>
```

Create a new self-signed CSR

```
openssl req -new -key <privatekey.key> -out request.csr -sha256
```

Verify CSR

```
openssl req -noout -text -in <cert_request.csr>
```

Convert DER to PEM format

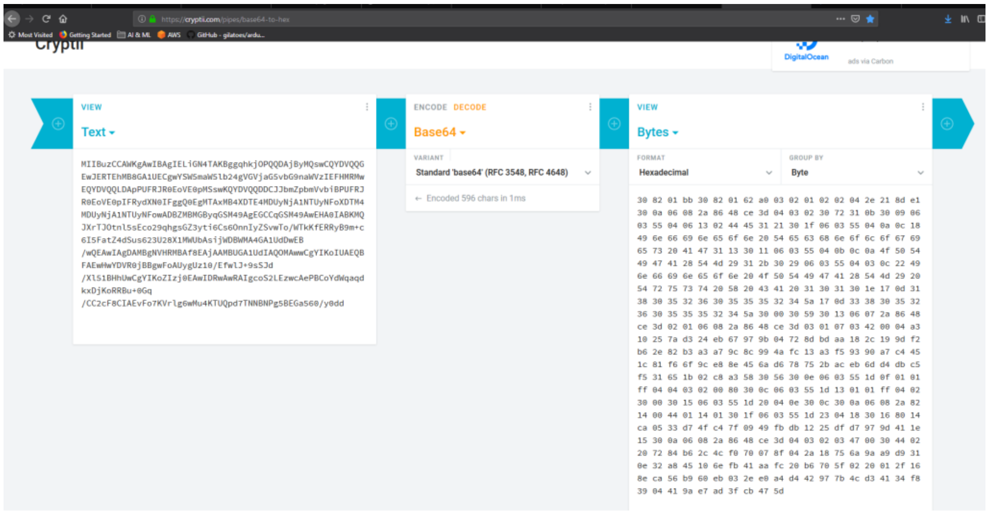
```
openssl x509 –inform der –in <cert.der> –out <cert.pem>
```

Convert PEM to DER format

```
openssl x509 –outform der –in <cert.pem> –out <cert.der>
```

Data Conversion

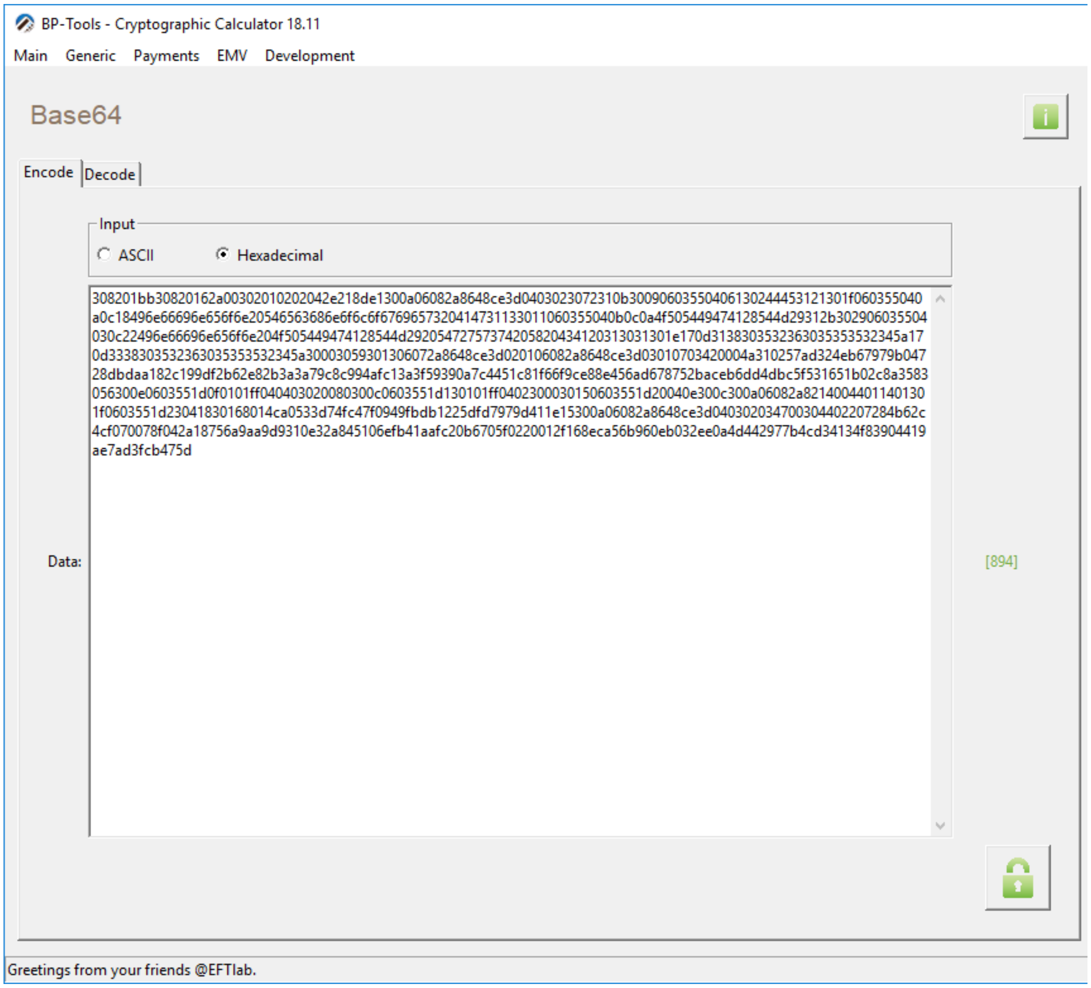
Website such as https://crytii.com can be used to convert hex to base64



```
MIIBuzCCAWKgAwIBAgIELiGN4TAKBggqhkjOPQQDAjByMQswCQYDVQQG
EwJERTEhMB8GA1UECgwYSW5maW5lb24gVGVjaG5vbG9naWVzIEFHMRMw
EQYDVQQLDApPUFRJR0EoVE0pMSswKQYDVQQDDCJJbmZpbmVvbiBPUFRJ
R0EoVE0pIFRydXN0IFggQ0EgMTAxMB4XDTE4MDUyNjA1NTUyNFoXDTM4
MDUyNjA1NTUyNFowADBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKMQ
JXrTJOtnl5sEco29qhgsGZ3yti6Cs6OnnIyZSvwTo/WTkKfERRyB9m+c
6I5FatZ4dSus623U28X1MWUbAsijWDBWMA4GA1UdDwEB
/wQEAwIAgDAMBgNVHRMBAf8EAjAAMBUGA1UdIAQOMAwwCgYIKoIUAEQB
FAEwHwYDVR0jBBgwFoAUygUz10/EfwlJ+9s5Jd
/Xl51BHhUwCgYIKoZIzj0EAwIDRwAwRAIgcoS2LEzwcAePBCoYdWqaqd
kxDjKoRRBu+0Gq
/CC2cF8CIAEvFo7KVrlg6wMu4KTUQpd7TNNBNPg5BEGa560/y0dd
```

```
30 82 01 bb 30 82 01 62 a0 03 02 01 02 02 04 2e 21 8d e1
30 0a 06 08 2a 86 48 ce 3d 04 03 02 30 72 31 0b 30 09 06
03 55 04 06 13 02 44 45 31 21 30 1f 06 03 55 04 0a 0c 18
49 6e 66 69 6e 65 6f 6e 20 54 65 63 68 6e 6f 6c 6f 67 69
65 73 20 41 47 31 13 30 11 06 03 55 04 0b 0c 0a 4f 50 54
49 47 41 28 54 4d 29 31 2b 30 29 06 03 55 04 03 0c 22 49
6e 66 69 6e 65 6f 6e 20 4f 50 54 49 47 41 28 54 4d 29 20
54 72 75 73 74 20 58 20 43 41 20 31 30 31 30 1e 17 0d 31
38 30 35 32 36 30 35 35 35 32 34 5a 17 0d 33 38 30 35 32
36 30 35 35 35 32 34 5a 30 00 30 59 30 13 06 07 2a 86 48
ce 3d 02 01 06 08 2a 86 48 ce 3d 03 01 07 03 42 00 04 a3
10 25 7a d3 24 eb 67 97 9b 04 72 8d bd aa 18 2c 19 9d f2
b6 2e 82 b3 a3 a7 9c 8c 99 4a fc 13 a3 f5 93 90 a7 c4 45
1c 81 f6 6f 9c e8 8e 45 6a d6 78 75 2b ac eb 6d d4 db c5
f5 31 65 1b 02 c8 a3 58 30 56 30 0e 06 03 55 1d 0f 01 01
ff 04 04 03 02 00 80 30 0c 06 03 55 1d 13 01 01 ff 04 02
30 00 30 15 06 03 55 1d 20 04 0e 30 0c 30 0a 06 08 2a 82
14 00 44 01 14 01 30 1f 06 03 55 1d 23 04 18 30 16 80 14
ca 05 33 d7 4f c4 7f 09 49 fb db 12 25 df d7 97 9d 41 1e
15 30 0a 06 08 2a 86 48 ce 3d 04 03 02 03 47 00 30 44 02
20 72 84 b6 2c 4c f0 70 07 8f 04 2a 18 75 6a 9a a9 d9 31
0e 32 a8 45 10 6e fb 41 aa fc 20 b6 70 5f 02 20 01 2f 16
8e ca 56 b9 60 eb 03 2e e0 a4 d4 42 97 7b 4c d3 41 34 f8
39 04 41 9a e7 ad 3f cb 47 5d
```

BP Tools

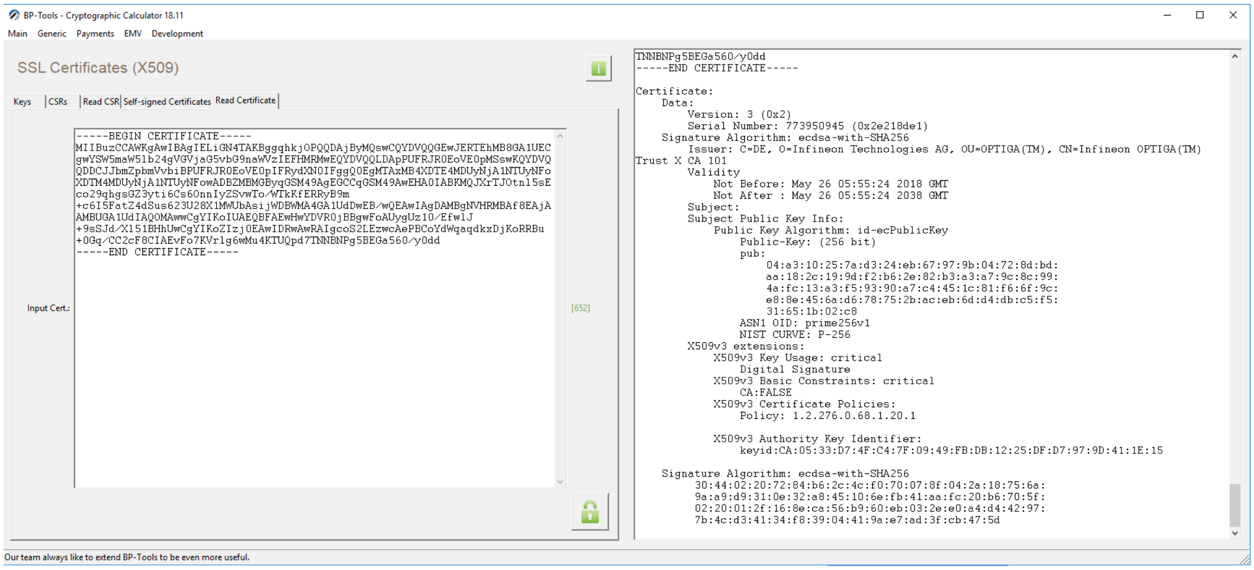


○ ASCII ● Hexadecimal

```
308201bb30820162a00302010202042e218de1300a06082a8648ce3d0403023072310b30090603550406130244453121301f060355040
a0c18496e66696e656f6e20546563686e6f6c6f6769657320414731133011060355040b0c0a4f505449474128544d29312b302906035504
030c22496e66696e656f6e204f505449474128544d2920547275737420582043412031303130 1e170d3138303532363035353532345a17
0d3338303532363035353532345a3000305930130607 2a8648ce3d020106082a8648ce3d03010703420004a310257ad324eb67979b047
28dbdaa182c199df2b62e82b3a3a79c8c994afc13a3f59390a7c4451c81f66f9ce88e456ad678752baceb6dd4dbc5f531651b02c8a3583
056300e0603551d0f0101ff040403020080300c0603551d130101ff04023000301506 03551d20040e300c300a06082a8214004401140130
1f0603551d23041830168014ca0533d74fc47f0949fbdb1225dfd7979d411e15300a06082a8648ce3d0403020347003044022072 84b62c
4cf070078f042a18756a9aa9d9310e32a845106efb41aafc20b6705f0220012f168eca56b960eb032ee0a4d442977b4cd34134f83904419
ae7ad3fcb475d
```

Greetings from your friends @EFTlab.

Certificate Tool


BP-Tools - Cryptographic Calculator 18.11
Main Generic Payments EMV Development
SSL Certificates (X509)
Keys CSRs Read CSR Self-signed Certificates Read Certificate
Input Cert.:
[652]
Our team always like to extend BP-Tools to be even more useful.

```
-----BEGIN CERTIFICATE-----
MIIBuzCCAWKgAwIBAgIELiGN4TAKBggqhkjOPQQDAjByMQswCQYDVQQGEwJERTEhMB8GA1UEC
gwYSW5maW5lb24gVGVjaG5vbG9naWVzIEFHMRMwEQYDVQQLDApPUFRJR0EoVE0pMSswKQYDVQ
QDDCJJbmZpbmVvbiBPUFRJR0EoVE0pIFRydXN0IFggQ0EgMTAxMB4XDTE4MDUyNjA1NTUyNFo
XDTM4MDUyNjA1NTUyNFowADBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABKMQJXrTJOtnl5sE
co29qhgsGZ3yti6Cs6OnnIyZSvwTo/WTkKfERRyB9m
+c6I5FatZ4dSus623U28X1MWUbAsijWDBWMA4GA1UdDwEB/wQEAwIAgDAMBgNVHRMBAf8EAjA
AMBUGA1UdIAQOMAwwCgYIKoIUAEQBFAEwHwYDVR0jBBgwFoAUygUz10/EfwlJ
+9sSJd/Xl51BHhUwCgYIKoZIzj0EAwIDRwAwRAIgcoS2LEzwcAePBCoYdWqaqdkxDjKoRRBu
+0Gq/CC2cF8CIAEvFo7KVrlg6wMu4KTUQpd7TNNBNPg5BEGa560/y0dd
-----END CERTIFICATE-----
```

```
TNNBNPg5BEGa560/y0dd
-----END CERTIFICATE-----

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 773950945 (0x2e218de1)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=DE, O=Infineon Technologies AG, OU=OPTIGA(TM), CN=Infineon OPTIGA(TM)
Trust X CA 101
        Validity
            Not Before: May 26 05:55:24 2018 GMT
            Not After : May 26 05:55:24 2038 GMT
        Subject:
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:a3:10:25:7a:d3:24:eb:67:97:9b:04:72:8d:bd:
                    aa:18:2c:19:9d:f2:b6:2e:82:b3:a3:a7:9c:8c:99:
                    4a:fc:13:a3:f5:93:90:a7:c4:45:1c:81:f6:6f:9c:
                    e8:8e:45:6a:d6:78:75:2b:ac:eb:6d:d4:db:c5:f5:
                    31:65:1b:02:c8
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Certificate Policies:
                Policy: 1.2.276.0.68.1.20.1

            X509v3 Authority Key Identifier:
                keyid:CA:05:33:D7:4F:C4:7F:09:49:FB:DB:12:25:DF:D7:97:9D:41:1E:15

    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:72:84:b6:2c:4c:f0:70:07:8f:04:2a:18:75:6a:
         9a:a9:d9:31:0e:32:a8:45:10:6e:fb:41:aa:fc:20:b6:70:5f:
         02:20:01:2f:16:8e:ca:56:b9:60:eb:03:2e:e0:a4:d4:42:97:
         7b:4c:d3:41:34:f8:39:04:41:9a:e7:ad:3f:cb:47:5d
```

Mission:

	Public Key (68 Bytes)
My Generated Key (Provision Process) **Important: Disable provision me after generating the key**	
Exchanged Public key	
Calculated Share Secret	
Derived Secret	