Encryption and Decryption test

- Encryption process on Android

```
        ConfigManager.init("jar://jdigidoc.cfg");
       Log.d("despues de:", "ConfigManager.init");

           /** signed doc object if used */
           SignedDoc m_sdoc;
           m_sdoc = null;

           /** encrypted data object if used */
           EncryptedData m_cdoc;
           m_cdoc = null;

           String inFile = null, outFile = null;
           String certFile = null;
           String recipient = null;
           String keyName = null;
           String carriedKeyName = null;
           String sId = null;

           inFile = str;


           outFile = "cifrado.cdoc";

           certFile = "/mnt/sdcard/chespirito.crt";


           // agregar el destinatario
           try {
                   if (m_cdoc == null){
                           Log.d("m_cdoc == null", "-");
                           m_cdoc = new EncryptedData(null, null, null, EncryptedData.DENC_XMLNS_XMLENC, EncryptedData.DEN
                   }
                   Log.d("Adding recipient", certFile);
                   X509Certificate recvCert = SignedDoc.readCertificate(new File(certFile));
                   if (recvCert != null && recipient == null)
                           recipient = SignedDoc.getCommonName(recvCert.getSubjectDN().getName());
                   Log.d("Recipient", recipient);
                   if (sId == null){
                           int n = m_cdoc.getNumKeys() + 1;
                           sId = "ID" + n;

                   }

                   EncryptedKey ekey = new EncryptedKey(sId, recipient, EncryptedData.DENC_ENC_METHOD_RSA1_5, keyName, car
                   m_cdoc.addEncryptedKey(ekey);


           }catch(Exception e){
                   Log.d("Error adding EncryptedKey: ", e.getMessage());
                   Toast.makeText(getApplicationContext(), e.getMessage(), Toast.LENGTH_SHORT).show();
           }

           // ejecutar el cifrado
           try {
                   Log.d("Encrypting file:", inFile + " to: " + outFile);
                   File fIn = new File(inFile);
                   // create a ddoc intermediate file
```

```
                m_sdoc = new SignedDoc(SignedDoc.FORMAT_DIGIDOC_XML, SignedDoc.VERSION_1_3);

                Log.d("Encrypting file:", "paso new SignedDoc");

                DataFile df = m_sdoc.addDataFile(new File(inFile), SignedDoc.xmlns_digidoc13, DataFile.CONTENT_EMBEDDED

                Log.d("Encrypting file:", "paso addDataFile");


                byte[] data = SignedDoc.readFile(new File(inFile));

                Log.d("Encrypting file:", "paso readFile");

                df.setBase64Body(data);

                Log.d("Encrypting file:", "paso setBase64Body");

                byte[] inData = m_sdoc.toXML().getBytes("UTF-8");

                Log.d("Encrypting file:", "paso toXML()");

                Log.d("Encrypting file", "Content: " + inFile + " size: " + data.length);
                Log.d("Encrypting file", "DF: " + new String(inData));

                m_cdoc.setData(inData);
                m_cdoc.setDataStatus(EncryptedData.DENC_DATA_STATUS_UNENCRYPTED_AND_NOT_COMPRESSED);
                m_cdoc.addProperty(EncryptedData.ENCPROP_FILENAME, inFile + ".ddoc");
                m_cdoc.setMimeType(EncryptedData.DENC_ENCDATA_TYPE_DDOC);
                StringBuffer sb = new StringBuffer();
                sb.append(fIn.getName());
                sb.append("|");
                sb.append(new Long(fIn.length()).toString() + " B|");
                sb.append("application/unknown|");
                sb.append("/" + fIn.getName());
                m_cdoc.addProperty(EncryptedData.ENCPROP_ORIG_FILE, sb.toString());
                //m_cdoc.addProperty(EncryptedData.ENCPROP_ORIG_SIZE, new Long(inData.length).toString());

                int nCompressOption = 0;

                m_cdoc.encrypt(nCompressOption);


                // genera el archivo cifrado en /data/data/ve.gob.cenditel/files
                FileOutputStream fos = openFileOutput(outFile, Context.MODE_PRIVATE);

                Log.d("Encrypting file", "antes de escribir archivo " + outFile);

                fos.write(m_cdoc.toXML());

                Log.d("Encrypting file", "despues de escribir archivo " + outFile);

                fos.close();

                Log.d("Encrypting file", "despues de cerrar archivo " + outFile);

                Toast.makeText(getApplicationContext(), "Cifrado correctamente: " + outFile, Toast.LENGTH_SHORT).show()


        } catch(Exception e) {
                Log.d("Error encrypting file: ", inFile + " - " + e.getMessage());
                e.printStackTrace(System.err);
```

```
                    Toast.makeText(getApplicationContext(), e.getMessage(), Toast.LENGTH_SHORT).show();
            }
```

- Decryption process with jdigidocutil (encrypted file through Android)

```
aaraujo@moe:~/desarrollo/andriod/pruebas/jdigidoc-3.7/jdigidoc$ java -jar jdigidocutil-\$\{version\}.jar -cdoc-in /tmp/cif
JDigiDoc - 3.6.0.1
Reading config file: jar://jdigidoc.cfg
Reading encrypted file: /tmp/cifrado.cdoc
Decrypting to: /tmp/salida.pdf
Using recipient: 0
SAXDigiDocFactory::readSignedDocOfType
Start reading ddoc/bdoc from file: /tmp/salida.pdf
Start Element: SignedDoc lname:  uri:
Start Element: DataFile lname:  uri:
Start collecting digest
Allocating buf: 122556 Element: DataFile lname:  uri:
Attr: ContentType ='EMBEDDED_BASE64'
Attr: Filename ='LSMDFE.pdf'
Attr: Id ='D0'
Attr: MimeType ='http://www.sk.ee/DigiDoc/v1.3.0#'
Attr: Size ='61278'
Attr: xmlns ='http://www.sk.ee/DigiDoc/v1.3.0#'
Canonicalized: '<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#" ContentType="EMBEDDED_BASE64" Filename="LSMDFE.pdf" Id=
End Element: DataFile collect: 1
Digest: D0 - 5hmr2x1Q4PKrjbmkWy7K+jzYL/o= size: 61278
End Element: SignedDoc collect: 0
JDigiDoc end, time: 3 sec result: success
```

An example of a file without xmlns prefix

```
<?xml version="1.0" encoding="UTF-8" ?><EncryptedData MimeType="http://www.isi.edu/in-noes/iana/assignments/media-types/ap
DzANBgNVBAgTBk1lcmlkYTEPMA0GA1UEBxMGTWVyaWRhMREwDwYDVQQKEwhDRU5E
SVRFTDEOMAwGA1UECxMFR0lEU0kxLjAsBgNVBAMMJUF1dG9yaWRhZCBkZSBDZXJ0
aWZpY2FjacOzbiBkZWwgR0lEU0kxJjAkBgkqhkiG9w0BCQEWF2FjZ2lkc2lAY2Vu
ZGl0ZWwuZ29iLnZlMB4XDTEyMDQyNjE2MDUwMFoXDTEzMDQyNjE2MDUwMFowgZYx
CzAJBgNVBAYTAk1YMRIwEAYDVQQIEwlNb250ZXJyZXkxEDAOBgNVBAcTB0phbGlz
Y28xETAPBgNVBAoTCENFTkRJVEVMMQ4wDAYDVQQLEwVHSURTSTETMBEGA1UEAxMK
Q2hlc3Bpcml0bzEpMCcGCSqGSIb3DQEJARYaY2hlc3Bpcml0b0BjZW5kaXRlbC5n
b2IudmUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDNWsKCFNPW4Cxq
qduuzbMODqUbt7uSAxdnyLTpZ6P8cfwnberSzq/8X2kKTpuzScb2L4+0I4GxAaqu
td80XJInKBtcTqYpzMpb3HlPbEUr1l+BbkUQ4Jn4CnE60UNY9d4ebTEOyV4LcuRZ
/fjnapeFppWYrJ5kOjtRCGlbSl8azP4NCMhh6alrhW2JMwV6AmvQTgk2m8tzIDzO
fM9YcHuqU31ly2vzLbj+xc+oSevUftwdoEtU6bogCrXuDnBsEmPNqUacDk+o1zj8
vmWXYByTudsfKcG1zqwHtSOcK3neb9XU8gNCLPsZpNnG2tGT3FfUZTn7zi6YRcD2
OFJZ4rClAgMBAAGjbzBtMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgTwMBEGCWCG
SAGG+EIBAQQEAwIFoDAeBglghkgBhvhCAQ0EERYPeGNhIGNlcnRpZmljYXRlMB0G
A1UdDgQWBBRhVVfxfHWbQhFkC0qK0wkyonrTaTANBgkqhkiG9w0BAQsFAAOCAgEA
Xq9j6jVCt7zdwv0AAUpSdQtMR7bMnUvy3eu+C7omW/SZxrg4EYYgn0iI+rgj9A+O
0R0QcG4TgM5dnUtWae4PKqQEUH8tbc8jvERlD0gxXGDWU3KEXJ0UBDgmwr57eI9B
sOSG4Y4rKB/PEsrLUpODfY+rxDDPoU+R+8FdBzUl3QLsgAWPHkbWDLM7xpmMJiMx
umTckoGn8riv1FvJ16t4UJYqIsETdRpoIr51yQ0m+mzfKji/cgpo6HFG2f0BmC+G
G7ma1PWl2Liaf9Y8J+kmqp9aX1JHcAX7H7tpgC9KUxcmdWrzORaLjNTz2KjgcoWj
o/TWoQDH6vNXCZq5bInmvn4BARNAxaZQMEkp3K6uKlgHJwKfHwsxf68xnC9InMV+
mfQWA1Ls3UbHm6gZjDxQL4a8y6NCB66RbYBFJRWh56aY/FxEbZ4gNwkFiEZO3Yxg
hv21gJyBvh89l2uExyOZn4WJUrTBYlb348o4G9ZvXA3kfklG3B+rz+24qLS5iWm4
bsEkQg0nnuQmB1CTJTSavjbmzZ4gDavCdgXVHmeeLYoNLb1YUMSDt1pENCJ8BZR0
n4dQDUQiP8dIqmpoGK9R1wasxijb99QnQXDr++55nATijn1qcssqYV2c4R1b5Gri
```

```
0GlIiOlnCN9r1us1Icr+9vU4Z3qao4okTSQrVjSm/og=</X509Certificate></X509Data></KeyInfo><CipherData><CipherValue>lJmQmmDM4t4/OE
2lr7kCKxOmoMuiJqTPEwLg/5KFgm+1oBdP131sM8dYH3DC/3s82O5tyijpg1K7wW
i0Mp9dduIqlq+x1pdMZlTA76I3q+/gi29e8FNgDaSYToNTuD2xAXjeUDQrkDTjMR
kk6gzwQkQgwPDIbblSZtIuL+JbLDsoP9sYiSrQXUh1M2cSsOp7bfURCmXHDUv1GD
3ZtvwkFvJRJuFKkbEmn/xn4qHvP/GGDTJWLM145IX8O1eGLY1vJAe/vnYXx3UWHW
us62TufDpDgv3I0Knx8xOA==</CipherValue></CipherData></EncryptedKey></KeyInfo><CipherData><CipherValue>Mg++HduoRKVYMHCOqF9U0
9R/Mp7eoBkNi0eBoISIzTigpgHrMwJcEzcXhQPxfNsLrrTsuTHO60douVNbXzxvg
hR4dv1Dd3QZDAe6xK/COEQKukiRbVlys3i6B9427yFnAHs5Y3d8vLMbHdpeu3W8x
Pw/N3QPWgtoSujsdQ8y6u/ZFnyxFaUbIgNFdC7vhY/xAhSRE7mTHalvm8s45xjIZ
8eX7pyxK56KjtBIjZWw8ZPjFBZEOh33tfefXBycUOz6MUni/9zdgmF2HjfYiATkx
affu3uaKYBKjz6QXcB/rJFKbJPMa8TyDZ+Sm4eq9gfDOkrJy3rLjm14s4722BUfM
zecLg01zDa40p5iTutQZsRODbRznwQ+/swe27xhUrbZj5Gk86w+OP/hLN2YEsrjw
BkFsJD4Z1+aBFrvlk9bSrHIFvBqB+PnrxENObF3M2m8p9anZzNdfXA/mRobHfvG3
6J+tTDMA4sBJyhOd+NgRBcZdSQB/CF8dmma2gZL+vGIsPwfKiambiRs2Vzm0tKMx
c1F/13tUQ71qmjVgKGDR9yx59JKD3OxYw3N3TQFUmoCc59U+4djWFUt/A3OQTC48
pSGfKNodGEChFtR/ks8Vbq1vqAP0fs9WEXs1XctqZjIaR9TG7NJoP4Y/i+Ldu+jB
zuikaV0uXmrNOtK27Z0IZS1reOPoe9496VxMHFX+fTrUF7yb877AyCSPAENHVCrY
inU4cItIyKmbly0001VaAmOgiTI1jfF4nIJp6yG5CJydet0/p5kPkXi7hpX4iBzH
uuUnBvvZdcUz7oSssiea/GBNxus2B+EdFI2LeE8Tg67SKSQUD/CpgdOdj6x8n7gv
FgULByAM3Rv2NUfNBIug9dQPY99tqYt3FYTgonethmB2h89q1YnYbKoeLXnrIQRx
dSq8CXBcdREHC3zsmqXv4cjkrqVQiz6CeGPMyzJbeXJDo0ZtiZWBf1x7TOSI8FfY
wWS3FMgIoEUCh0+ZtwI9fK9HJn5BqtCRVHXc5OmJli81sPmMUkgvwGvaSNodPv40
/5Tour5aPwXMaMJB8XTKmxK7xrxkMGCGiC6R0q9B6R4VDsj/nevqKpRAQGEF7+G3
SyLrLRSruZ30WhszIgBrsSgiH8VoiZHLKUOdHgW0kAO7S+3q2UlDAxAidgCgTD5S
eqeYjBImf2dTQ+B6fokeqfzZ1sbFEdjDnv+YjAY5i2aNIhqzlbE4cX7JgNu497Bn
lzOI27UB51ExbyJ68Lvm0K3yKpyMn8KgS0haYkWIGAl2Q7u1wKd2skyW6eKbQ66y
aZu+oouotxMAMLco6dL/gjezTpiCWUILomYi4Ud6Hmk6ExmqAjccNziQueBEHT07
OMet5nWv2D4KVVh9+2+gZw==</CipherValue></CipherData><EncryptionProperties><EncryptionProperty Name="LibraryVersion">JDigiDo
```

java.security.InvalidKeyException?: Key length not 128/192/256 bits

```
...
06-19 11:26:29.627: D/dalvikvm(13190): GC_CONCURRENT freed 980K, 52% free 3441K/7047K, external 2058K/2137K, paused 3ms+3m
06-19 11:26:30.967: I/System.out(13190): EncryptedData.java: decryptPkcs12 Decrypting key: 0 with token: 0
06-19 11:26:30.967: I/System.out(13190): loading key: Chespirito passwd-len: 10
06-19 11:26:30.967: I/System.out(13190): Key: OK, algorithm: RSA
06-19 11:26:31.217: I/System.out(13190): Decrypted len: 255
06-19 11:26:31.227: I/System.out(13190): decryptWithKey: Decrypting 57728 using iv 16 left: 57712
06-19 11:26:31.227: I/System.out(13190): deckey pos: 0 = 2
06-19 11:26:31.227: I/System.out(13190): deckey pos: 1 = -64
06-19 11:26:31.227: I/System.out(13190): deckey pos: 2 = -79
06-19 11:26:31.227: I/System.out(13190): deckey pos: 3 = 95
06-19 11:26:31.227: I/System.out(13190): deckey pos: 4 = -17
06-19 11:26:31.227: I/System.out(13190): deckey pos: 5 = 96
06-19 11:26:31.227: I/System.out(13190): deckey pos: 6 = 60
06-19 11:26:31.227: I/System.out(13190): deckey pos: 7 = 116
06-19 11:26:31.227: I/System.out(13190): deckey pos: 8 = 102
06-19 11:26:31.227: I/System.out(13190): deckey pos: 9 = 114
06-19 11:26:31.227: I/System.out(13190): deckey pos: 10 = -77
06-19 11:26:31.227: I/System.out(13190): deckey pos: 11 = 106
06-19 11:26:31.227: I/System.out(13190): deckey pos: 12 = 21
06-19 11:26:31.227: I/System.out(13190): deckey pos: 13 = -111
06-19 11:26:31.227: I/System.out(13190): deckey pos: 14 = 42
06-19 11:26:31.227: I/System.out(13190): deckey pos: 15 = 27
06-19 11:26:31.257: I/System.out(13190): deckey pos: 16 = -57
06-19 11:26:31.257: I/System.out(13190): deckey pos: 17 = 22
06-19 11:26:31.267: I/System.out(13190): deckey pos: 18 = -10
06-19 11:26:31.267: I/System.out(13190): deckey pos: 19 = 34
06-19 11:26:31.277: I/System.out(13190): deckey pos: 20 = -71
06-19 11:26:31.277: I/System.out(13190): deckey pos: 21 = -98
```

```
06-19 11:26:31.277: I/System.out(13190): deckey pos: 22 = -61
06-19 11:26:31.277: I/System.out(13190): deckey pos: 23 = -3
06-19 11:26:31.277: I/System.out(13190): deckey pos: 24 = -9
06-19 11:26:31.300: I/System.out(13190): deckey pos: 25 = 125
06-19 11:26:31.300: I/System.out(13190): deckey pos: 26 = -93
06-19 11:26:31.308: I/System.out(13190): deckey pos: 27 = 73
06-19 11:26:31.308: I/System.out(13190): deckey pos: 28 = 81
06-19 11:26:31.308: I/System.out(13190): deckey pos: 29 = 11
06-19 11:26:31.308: I/System.out(13190): deckey pos: 30 = -97
06-19 11:26:31.308: I/System.out(13190): deckey pos: 31 = 99
06-19 11:26:31.308: I/System.out(13190): deckey pos: 32 = 93
06-19 11:26:31.308: I/System.out(13190): deckey pos: 33 = -81
06-19 11:26:31.308: I/System.out(13190): deckey pos: 34 = -36
06-19 11:26:31.308: I/System.out(13190): deckey pos: 35 = 51
06-19 11:26:31.317: I/System.out(13190): deckey pos: 36 = 99
06-19 11:26:31.317: I/System.out(13190): deckey pos: 37 = 11
06-19 11:26:31.317: I/System.out(13190): deckey pos: 38 = -14
06-19 11:26:31.317: I/System.out(13190): deckey pos: 39 = -120
06-19 11:26:31.317: I/System.out(13190): deckey pos: 40 = 8
06-19 11:26:31.317: I/System.out(13190): deckey pos: 41 = -117
06-19 11:26:31.317: I/System.out(13190): deckey pos: 42 = 91
06-19 11:26:31.317: I/System.out(13190): deckey pos: 43 = 16
06-19 11:26:31.317: I/System.out(13190): deckey pos: 44 = 54
06-19 11:26:31.317: I/System.out(13190): deckey pos: 45 = -5
06-19 11:26:31.317: I/System.out(13190): deckey pos: 46 = 24
06-19 11:26:31.317: I/System.out(13190): deckey pos: 47 = -80
06-19 11:26:31.327: I/System.out(13190): deckey pos: 48 = 69
06-19 11:26:31.327: I/System.out(13190): deckey pos: 49 = 80
06-19 11:26:31.327: I/System.out(13190): deckey pos: 50 = -1
06-19 11:26:31.327: I/System.out(13190): deckey pos: 51 = 7
06-19 11:26:31.327: I/System.out(13190): deckey pos: 52 = -78
06-19 11:26:31.327: I/System.out(13190): deckey pos: 53 = 22
06-19 11:26:31.327: I/System.out(13190): deckey pos: 54 = 124
06-19 11:26:31.327: I/System.out(13190): deckey pos: 55 = -15
06-19 11:26:31.327: I/System.out(13190): deckey pos: 56 = -128
06-19 11:26:31.327: I/System.out(13190): deckey pos: 57 = 75
06-19 11:26:31.327: I/System.out(13190): deckey pos: 58 = 73
06-19 11:26:31.327: I/System.out(13190): deckey pos: 59 = -32
06-19 11:26:31.337: I/System.out(13190): deckey pos: 60 = -46
06-19 11:26:31.337: I/System.out(13190): deckey pos: 61 = -103
06-19 11:26:31.337: I/System.out(13190): deckey pos: 62 = 67
06-19 11:26:31.337: I/System.out(13190): deckey pos: 63 = 115
06-19 11:26:31.337: I/System.out(13190): deckey pos: 64 = 108
06-19 11:26:31.337: I/System.out(13190): deckey pos: 65 = 119
06-19 11:26:31.337: I/System.out(13190): deckey pos: 66 = -96
06-19 11:26:31.337: I/System.out(13190): deckey pos: 67 = 23
06-19 11:26:31.337: I/System.out(13190): deckey pos: 68 = 98
06-19 11:26:31.337: I/System.out(13190): deckey pos: 69 = 44
06-19 11:26:31.337: I/System.out(13190): deckey pos: 70 = 9
06-19 11:26:31.337: I/System.out(13190): deckey pos: 71 = -113
06-19 11:26:31.337: I/System.out(13190): deckey pos: 72 = 86
06-19 11:26:31.337: I/System.out(13190): deckey pos: 73 = -91
06-19 11:26:31.337: I/System.out(13190): deckey pos: 74 = 121
06-19 11:26:31.337: I/System.out(13190): deckey pos: 75 = -56
06-19 11:26:31.347: I/System.out(13190): deckey pos: 76 = 59
06-19 11:26:31.347: I/System.out(13190): deckey pos: 77 = 105
06-19 11:26:31.347: I/System.out(13190): deckey pos: 78 = 119
06-19 11:26:31.347: I/System.out(13190): deckey pos: 79 = -107
06-19 11:26:31.347: I/System.out(13190): deckey pos: 80 = 60
06-19 11:26:31.347: I/System.out(13190): deckey pos: 81 = -111
06-19 11:26:31.347: I/System.out(13190): deckey pos: 82 = 88
```

```
06-19 11:26:31.347: I/System.out(13190): deckey pos: 83 = -68
06-19 11:26:31.347: I/System.out(13190): deckey pos: 84 = -42
06-19 11:26:31.347: I/System.out(13190): deckey pos: 85 = -28
06-19 11:26:31.347: I/System.out(13190): deckey pos: 86 = -14
06-19 11:26:31.347: I/System.out(13190): deckey pos: 87 = -113
06-19 11:26:31.347: I/System.out(13190): deckey pos: 88 = -97
06-19 11:26:31.357: I/System.out(13190): deckey pos: 89 = -112
06-19 11:26:31.357: I/System.out(13190): deckey pos: 90 = 53
06-19 11:26:31.357: I/System.out(13190): deckey pos: 91 = 112
06-19 11:26:31.357: I/System.out(13190): deckey pos: 92 = 120
06-19 11:26:31.357: I/System.out(13190): deckey pos: 93 = 126
06-19 11:26:31.357: I/System.out(13190): deckey pos: 94 = 92
06-19 11:26:31.357: I/System.out(13190): deckey pos: 95 = -84
06-19 11:26:31.368: I/System.out(13190): deckey pos: 96 = -46
06-19 11:26:31.368: I/System.out(13190): deckey pos: 97 = 22
06-19 11:26:31.368: I/System.out(13190): deckey pos: 98 = -1
06-19 11:26:31.376: I/System.out(13190): deckey pos: 99 = -104
06-19 11:26:31.376: I/System.out(13190): deckey pos: 100 = 4
06-19 11:26:31.376: I/System.out(13190): deckey pos: 101 = -82
06-19 11:26:31.376: I/System.out(13190): deckey pos: 102 = -9
06-19 11:26:31.376: I/System.out(13190): deckey pos: 103 = 41
06-19 11:26:31.376: I/System.out(13190): deckey pos: 104 = -77
06-19 11:26:31.376: I/System.out(13190): deckey pos: 105 = -37
06-19 11:26:31.387: I/System.out(13190): deckey pos: 106 = -122
06-19 11:26:31.387: I/System.out(13190): deckey pos: 107 = 9
06-19 11:26:31.387: I/System.out(13190): deckey pos: 108 = -110
06-19 11:26:31.387: I/System.out(13190): deckey pos: 109 = -84
06-19 11:26:31.387: I/System.out(13190): deckey pos: 110 = -105
06-19 11:26:31.387: I/System.out(13190): deckey pos: 111 = 19
06-19 11:26:31.387: I/System.out(13190): deckey pos: 112 = -25
06-19 11:26:31.387: I/System.out(13190): deckey pos: 113 = -97
06-19 11:26:31.397: I/System.out(13190): deckey pos: 114 = -25
06-19 11:26:31.397: I/System.out(13190): deckey pos: 115 = 20
06-19 11:26:31.397: I/System.out(13190): deckey pos: 116 = 14
06-19 11:26:31.397: I/System.out(13190): deckey pos: 117 = 11
06-19 11:26:31.397: I/System.out(13190): deckey pos: 118 = 35
06-19 11:26:31.397: I/System.out(13190): deckey pos: 119 = 41
06-19 11:26:31.407: I/System.out(13190): deckey pos: 120 = 13
06-19 11:26:31.407: I/System.out(13190): deckey pos: 121 = -19
06-19 11:26:31.407: I/System.out(13190): deckey pos: 122 = 72
06-19 11:26:31.407: I/System.out(13190): deckey pos: 123 = -93
06-19 11:26:31.407: I/System.out(13190): deckey pos: 124 = -125
06-19 11:26:31.407: I/System.out(13190): deckey pos: 125 = 92
06-19 11:26:31.407: I/System.out(13190): deckey pos: 126 = 120
06-19 11:26:31.407: I/System.out(13190): deckey pos: 127 = 75
06-19 11:26:31.407: I/System.out(13190): deckey pos: 128 = 107
06-19 11:26:31.416: I/System.out(13190): deckey pos: 129 = -2
06-19 11:26:31.416: I/System.out(13190): deckey pos: 130 = 89
06-19 11:26:31.427: I/System.out(13190): deckey pos: 131 = -108
06-19 11:26:31.427: I/System.out(13190): deckey pos: 132 = 9
06-19 11:26:31.427: I/System.out(13190): deckey pos: 133 = 101
06-19 11:26:31.427: I/System.out(13190): deckey pos: 134 = 66
06-19 11:26:31.427: I/System.out(13190): deckey pos: 135 = -22
06-19 11:26:31.427: I/System.out(13190): deckey pos: 136 = 40
06-19 11:26:31.427: I/System.out(13190): deckey pos: 137 = 109
06-19 11:26:31.427: I/System.out(13190): deckey pos: 138 = -5
06-19 11:26:31.427: I/System.out(13190): deckey pos: 139 = -91
06-19 11:26:31.427: I/System.out(13190): deckey pos: 140 = -117
06-19 11:26:31.437: I/System.out(13190): deckey pos: 141 = -12
06-19 11:26:31.437: I/System.out(13190): deckey pos: 142 = 82
06-19 11:26:31.437: I/System.out(13190): deckey pos: 143 = -68
```

```
06-19 11:26:31.437: I/System.out(13190): deckey pos: 144 = 23
06-19 11:26:31.437: I/System.out(13190): deckey pos: 145 = -125
06-19 11:26:31.437: I/System.out(13190): deckey pos: 146 = 112
06-19 11:26:31.437: I/System.out(13190): deckey pos: 147 = -117
06-19 11:26:31.437: I/System.out(13190): deckey pos: 148 = -69
06-19 11:26:31.437: I/System.out(13190): deckey pos: 149 = 65
06-19 11:26:31.437: I/System.out(13190): deckey pos: 150 = -26
06-19 11:26:31.437: I/System.out(13190): deckey pos: 151 = 110
06-19 11:26:31.437: I/System.out(13190): deckey pos: 152 = -31
06-19 11:26:31.437: I/System.out(13190): deckey pos: 153 = -59
06-19 11:26:31.437: I/System.out(13190): deckey pos: 154 = 2
06-19 11:26:31.437: I/System.out(13190): deckey pos: 155 = -11
06-19 11:26:31.437: I/System.out(13190): deckey pos: 156 = 21
06-19 11:26:31.437: I/System.out(13190): deckey pos: 157 = -69
06-19 11:26:31.447: I/System.out(13190): deckey pos: 158 = -48
06-19 11:26:31.447: I/System.out(13190): deckey pos: 159 = 107
06-19 11:26:31.447: I/System.out(13190): deckey pos: 160 = -108
06-19 11:26:31.447: I/System.out(13190): deckey pos: 161 = -13
06-19 11:26:31.457: I/System.out(13190): deckey pos: 162 = -3
06-19 11:26:31.457: I/System.out(13190): deckey pos: 163 = 126
06-19 11:26:31.457: I/System.out(13190): deckey pos: 164 = -5
06-19 11:26:31.457: I/System.out(13190): deckey pos: 165 = 53
06-19 11:26:31.457: I/System.out(13190): deckey pos: 166 = 116
06-19 11:26:31.457: I/System.out(13190): deckey pos: 167 = -127
06-19 11:26:31.457: I/System.out(13190): deckey pos: 168 = -6
06-19 11:26:31.457: I/System.out(13190): deckey pos: 169 = 26
06-19 11:26:31.457: I/System.out(13190): deckey pos: 170 = 38
06-19 11:26:31.467: I/System.out(13190): deckey pos: 171 = 27
06-19 11:26:31.467: I/System.out(13190): deckey pos: 172 = -76
06-19 11:26:31.467: I/System.out(13190): deckey pos: 173 = -122
06-19 11:26:31.467: I/System.out(13190): deckey pos: 174 = -111
06-19 11:26:31.467: I/System.out(13190): deckey pos: 175 = -9
06-19 11:26:31.467: I/System.out(13190): deckey pos: 176 = -83
06-19 11:26:31.467: I/System.out(13190): deckey pos: 177 = -95
06-19 11:26:31.467: I/System.out(13190): deckey pos: 178 = -120
06-19 11:26:31.467: I/System.out(13190): deckey pos: 179 = -1
06-19 11:26:31.477: I/System.out(13190): deckey pos: 180 = 118
06-19 11:26:31.477: I/System.out(13190): deckey pos: 181 = 34
06-19 11:26:31.477: I/System.out(13190): deckey pos: 182 = -108
06-19 11:26:31.477: I/System.out(13190): deckey pos: 183 = -107
06-19 11:26:31.477: I/System.out(13190): deckey pos: 184 = -85
06-19 11:26:31.477: I/System.out(13190): deckey pos: 185 = 97
06-19 11:26:31.477: I/System.out(13190): deckey pos: 186 = 110
06-19 11:26:31.477: I/System.out(13190): deckey pos: 187 = 109
06-19 11:26:31.487: I/System.out(13190): deckey pos: 188 = 92
06-19 11:26:31.487: I/System.out(13190): deckey pos: 189 = 105
06-19 11:26:31.487: I/System.out(13190): deckey pos: 190 = 121
06-19 11:26:31.487: I/System.out(13190): deckey pos: 191 = -75
06-19 11:26:31.487: I/System.out(13190): deckey pos: 192 = 27
06-19 11:26:31.487: I/System.out(13190): deckey pos: 193 = -56
06-19 11:26:31.487: I/System.out(13190): deckey pos: 194 = -100
06-19 11:26:31.487: I/System.out(13190): deckey pos: 195 = 20
06-19 11:26:31.487: I/System.out(13190): deckey pos: 196 = 32
06-19 11:26:31.487: I/System.out(13190): deckey pos: 197 = 11
06-19 11:26:31.487: I/System.out(13190): deckey pos: 198 = -31
06-19 11:26:31.497: I/System.out(13190): deckey pos: 199 = 14
06-19 11:26:31.497: I/System.out(13190): deckey pos: 200 = -99
06-19 11:26:31.497: I/System.out(13190): deckey pos: 201 = -72
06-19 11:26:31.497: I/System.out(13190): deckey pos: 202 = -94
06-19 11:26:31.497: I/System.out(13190): deckey pos: 203 = -81
06-19 11:26:31.497: I/System.out(13190): deckey pos: 204 = -40
```

```
06-19 11:26:31.497: I/System.out(13190): deckey pos: 205 = -12
06-19 11:26:31.497: I/System.out(13190): deckey pos: 206 = -121
06-19 11:26:31.497: I/System.out(13190): deckey pos: 207 = 106
06-19 11:26:31.497: I/System.out(13190): deckey pos: 208 = -43
06-19 11:26:31.507: I/System.out(13190): deckey pos: 209 = 91
06-19 11:26:31.507: I/System.out(13190): deckey pos: 210 = 39
06-19 11:26:31.507: I/System.out(13190): deckey pos: 211 = -110
06-19 11:26:31.507: I/System.out(13190): deckey pos: 212 = 53
06-19 11:26:31.507: I/System.out(13190): deckey pos: 213 = -65
06-19 11:26:31.507: I/System.out(13190): deckey pos: 214 = -48
06-19 11:26:31.507: I/System.out(13190): deckey pos: 215 = 125
06-19 11:26:31.507: I/System.out(13190): deckey pos: 216 = 33
06-19 11:26:31.507: I/System.out(13190): deckey pos: 217 = -24
06-19 11:26:31.507: I/System.out(13190): deckey pos: 218 = -69
06-19 11:26:31.507: I/System.out(13190): deckey pos: 219 = 99
06-19 11:26:31.518: I/System.out(13190): deckey pos: 220 = 97
06-19 11:26:31.518: I/System.out(13190): deckey pos: 221 = -44
06-19 11:26:31.518: I/System.out(13190): deckey pos: 222 = 83
06-19 11:26:31.518: I/System.out(13190): deckey pos: 223 = -57
06-19 11:26:31.518: I/System.out(13190): deckey pos: 224 = 58
06-19 11:26:31.518: I/System.out(13190): deckey pos: 225 = 44
06-19 11:26:31.518: I/System.out(13190): deckey pos: 226 = -12
06-19 11:26:31.518: I/System.out(13190): deckey pos: 227 = 94
06-19 11:26:31.527: I/System.out(13190): deckey pos: 228 = -81
06-19 11:26:31.527: I/System.out(13190): deckey pos: 229 = 98
06-19 11:26:31.527: I/System.out(13190): deckey pos: 230 = 105
06-19 11:26:31.527: I/System.out(13190): deckey pos: 231 = 73
06-19 11:26:31.527: I/System.out(13190): deckey pos: 232 = -52
06-19 11:26:31.527: I/System.out(13190): deckey pos: 233 = -18
06-19 11:26:31.527: I/System.out(13190): deckey pos: 234 = -46
06-19 11:26:31.527: I/System.out(13190): deckey pos: 235 = 109
06-19 11:26:31.527: I/System.out(13190): deckey pos: 236 = -92
06-19 11:26:31.527: I/System.out(13190): deckey pos: 237 = -45
06-19 11:26:31.527: I/System.out(13190): deckey pos: 238 = 0
06-19 11:26:31.527: I/System.out(13190): deckey pos: 239 = 63
06-19 11:26:31.537: I/System.out(13190): deckey pos: 240 = -71
06-19 11:26:31.537: I/System.out(13190): deckey pos: 241 = -81
06-19 11:26:31.537: I/System.out(13190): deckey pos: 242 = 85
06-19 11:26:31.537: I/System.out(13190): deckey pos: 243 = -26
06-19 11:26:31.537: I/System.out(13190): deckey pos: 244 = -53
06-19 11:26:31.537: I/System.out(13190): deckey pos: 245 = -9
06-19 11:26:31.537: I/System.out(13190): deckey pos: 246 = -106
06-19 11:26:31.537: I/System.out(13190): deckey pos: 247 = 20
06-19 11:26:31.547: I/System.out(13190): deckey pos: 248 = -88
06-19 11:26:31.547: I/System.out(13190): deckey pos: 249 = 51
06-19 11:26:31.547: I/System.out(13190): deckey pos: 250 = 33
06-19 11:26:31.547: I/System.out(13190): deckey pos: 251 = 53
06-19 11:26:31.547: I/System.out(13190): deckey pos: 252 = -111
06-19 11:26:31.547: I/System.out(13190): deckey pos: 253 = 17
06-19 11:26:31.557: I/System.out(13190): deckey pos: 254 = 82
06-19 11:26:31.557: I/System.out(13190): *-*-*- Longitud de byte clave de transporte: 255
06-19 11:26:31.557: I/System.out(13190): antes de getCipher(Cipher.DECRYPT_MODE, m_transportKey, ivdata)
06-19 11:26:31.577: W/System.err(13190): ERROR: decrypting file: ERROR: 111 - ERROR: 111ee.sk.digidoc.DigiDocException; ne
06-19 11:26:31.577: W/System.err(13190):         ERROR: 111 - ERROR: 111ee.sk.digidoc.DigiDocException; nested exception i
06-19 11:26:31.577: W/System.err(13190):         ERROR: 112 - ERROR: 112java.security.InvalidKeyException; nested exceptio
06-19 11:26:31.577: W/System.err(13190):         java.security.InvalidKeyException: Key length not 128/192/256 bits.
06-19 11:26:31.577: D/ERROR: decrypting file:(13190): ERROR: 111ee.sk.digidoc.DigiDocException; nested exception is:
06-19 11:26:31.577: D/ERROR: decrypting file:(13190):         ERROR: 111 - ERROR: 111ee.sk.digidoc.DigiDocException; neste
06-19 11:26:31.577: D/ERROR: decrypting file:(13190):         ERROR: 112 - ERROR: 112java.security.InvalidKeyException; ne
06-19 11:26:31.577: D/ERROR: decrypting file:(13190):         java.security.InvalidKeyException: Key length not 128/192/25
06-19 11:26:31.587: W/System.err(13190): ERROR: 111 - ERROR: 111ee.sk.digidoc.DigiDocException; nested exception is:
```

```
06-19 11:26:31.587: W/System.err(13190):         ERROR: 111 - ERROR: 111ee.sk.digidoc.DigiDocException; nested exception i
06-19 11:26:31.597: W/System.err(13190):         ERROR: 112 - ERROR: 112java.security.InvalidKeyException; nested exceptio
06-19 11:26:31.597: W/System.err(13190):         java.security.InvalidKeyException: Key length not 128/192/256 bits.
06-19 11:26:31.597: W/System.err(13190): ERROR: 111 - ERROR: 111ee.sk.digidoc.DigiDocException; nested exception is:
06-19 11:26:31.597: W/System.err(13190):         ERROR: 112 - ERROR: 112java.security.InvalidKeyException; nested exceptio
06-19 11:26:31.597: W/System.err(13190):         java.security.InvalidKeyException: Key length not 128/192/256 bits.
06-19 11:26:31.597: W/System.err(13190): ERROR: 112 - ERROR: 112java.security.InvalidKeyException; nested exception is:
06-19 11:26:31.607: W/System.err(13190):         java.security.InvalidKeyException: Key length not 128/192/256 bits.
06-19 11:26:31.607: W/System.err(13190): java.security.InvalidKeyException: Key length not 128/192/256 bits.
06-19 11:26:31.607: W/System.err(13190):         at org.bouncycastle.jce.provider.JCEBlockCipher.engineInit(JCEBlockCipher
06-19 11:26:31.607: W/System.err(13190):         at javax.crypto.Cipher.init(Cipher.java:607)
06-19 11:26:31.607: W/System.err(13190):         at javax.crypto.Cipher.init(Cipher.java:557)
06-19 11:26:31.607: W/System.err(13190):         at ee.sk.xmlenc.EncryptedData.getCipher(EncryptedData.java:1000)
06-19 11:26:31.607: W/System.err(13190):         at ee.sk.xmlenc.EncryptedData.decryptWithKey(EncryptedData.java:1325)
06-19 11:26:31.617: W/System.err(13190):         at ee.sk.xmlenc.EncryptedData.decryptPkcs12(EncryptedData.java:1194)
06-19 11:26:31.617: W/System.err(13190):         at ve.gob.cenditel.tibisay.MainActivity.decryptFile(MainActivity.java:578
06-19 11:26:31.617: W/System.err(13190):         at ve.gob.cenditel.tibisay.MainActivity.onActivityResult(MainActivity.jav
06-19 11:26:31.617: W/System.err(13190):         at android.app.Activity.dispatchActivityResult(Activity.java:3908)
06-19 11:26:31.617: W/System.err(13190):         at android.app.ActivityThread.deliverResults(ActivityThread.java:2528)
06-19 11:26:31.617: W/System.err(13190):         at android.app.ActivityThread.handleSendResult(ActivityThread.java:2574)
06-19 11:26:31.617: W/System.err(13190):         at android.app.ActivityThread.access$2000(ActivityThread.java:117)
06-19 11:26:31.617: W/System.err(13190):         at android.app.ActivityThread$H.handleMessage(ActivityThread.java:961)
06-19 11:26:31.617: W/System.err(13190):         at android.os.Handler.dispatchMessage(Handler.java:99)
06-19 11:26:31.627: W/System.err(13190):         at android.os.Looper.loop(Looper.java:123)
06-19 11:26:31.627: W/System.err(13190):         at android.app.ActivityThread.main(ActivityThread.java:3683)
06-19 11:26:31.627: W/System.err(13190):         at java.lang.reflect.Method.invokeNative(Native Method)
06-19 11:26:31.627: W/System.err(13190):         at java.lang.reflect.Method.invoke(Method.java:507)
06-19 11:26:31.637: W/System.err(13190):         at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.
06-19 11:26:31.637: W/System.err(13190):         at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:597)
06-19 11:26:31.637: W/System.err(13190):         at dalvik.system.NativeStart.main(Native Method)
06-19 11:31:23.467: D/SntpClient(61): request time failed: java.net.SocketException: Address family not supported by proto
```