Key generation fails with EC after updating security provider on Android Kitkat and Lollipop

Infeasible Bug P2 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION [Deleted User] created issue #1 Sep 6, 2018 01:16AM

Hi guys,

After updating the security provider (https://developer.android.com/training/articles/security-gms-provider) on my applications MainActivity.onCreate() method:

```
try {
   ProviderInstaller.installIfNeeded(getApplicationContext());
} catch (GooglePlayServicesRepairableException | GooglePlayServicesNotAvailableException e) {
   throw new RuntimeException("FATAL ERROR: " + e.getMessage());
}
```

during the key generation on Android 4.4 the following exception is thrown and key generation fails:

```
java.lang.IllegalStateException: Can't generate certificate
      at android.security.AndroidKeyPairGenerator.generateKeyPair(AndroidKeyPairGenerator.java:137)
      at java.security.KeyPairGenerator$KeyPairGeneratorImpl.generateKeyPair(KeyPairGenerator.java:275)
...
    Caused by: java.lang.RuntimeException: error:100C0043:elliptic curve routines:i2d_ECPrivateKey:passed a
null parameter
      at com.android.org.conscrypt.NativeCrypto.i2d_PKCS8_PRIV_KEY_INFO(Native Method)
      at com.android.org.conscrypt.OpenSSLECPrivateKey.getEncoded(OpenSSLECPrivateKey.java:86)
      at
com.google.android.gms.org.conscrypt.OpenSSLKey.fromPrivateKey(:com.google.android.gms@12874004@12
.8.74 (000308-204998136):3)
      at
com.google.android.gms.org.conscrypt.OpenSSLSignature.engineInitSign(:com.google.android.gms@1287400
4@12.8.74 (000308-204998136))
      at java.security.Signature$SignatureImpl.engineInitSign(Signature.java:631)
      at java.security.Signature.initSign(Signature.java:280)
      at com.android.org.bouncycastle.x509.X509Util.calculateSignature(X509Util.java:257)
      at
com.android.org.bouncycastle.x509.X509V3CertificateGenerator.generate(X509V3CertificateGenerator.java:43
4)
```

during the key generation on Android 5.0 the following exception is thrown and the application crashes:

```
E/NativeCrypto: Could not sign message in EcdsaMethodDoSign!
A/art: sart/runtime/check_jni.cc:65] JNI DETECTED ERROR IN APPLICATION: JNI FindClass called with pending
exception 'java.lang.UnsupportedOperationException' thrown in unknown throw location
   sart/runtime/check_jni.cc:65]    in call to FindClass
   sart/runtime/check_jni.cc:65]    from byte[]
com.google.android.gms.org.conscrypt.NativeCrypto.EVP_DigestSignFinal(com.google.android.gms.org.conscr
ypt.NativeRef$EVP_MD_CTX)
   sart/runtime/check_jni.cc:65] "AsyncTask #6" prio=5 tid=24 Runnable
   sart/runtime/check_jni.cc:65]   | group="main" sCount=0 dsCount=0 obj=0x1329abe0 self=0x7fa1a2a000
   sart/runtime/check_jni.cc:65]   | sysTid=15147 nice=10 cgrp=apps/bg_non_interactive sched=0/0
handle=0x7faaf2e200
   sart/runtime/check_jni.cc:65]   | state=R schedstat=( 0 0 0 ) utm=35 stm=3 core=5 HZ=100
   sart/runtime/check_jni.cc:65]   | stack=0x7f71c55000-0x7f71c57000 stackSize=1036KB
   sart/runtime/check_jni.cc:65]   | held mutexes= "mutator lock"(shared held)
   sart/runtime/check_jni.cc:65]   native: #00 pc 0000435c  /system/lib64/libbacktrace_libc++.so
(Backtrace::Unwind(unsigned long, ucontext*)+28)
   sart/runtime/check_jni.cc:65]   native: #01 pc 00000027  ???
   sart/runtime/check_jni.cc:65]   native: #02 pc 0007bcfc  /system/lib64/libc++.so (operator new(unsigned
long)+40)
   sart/runtime/check_jni.cc:65]   at
com.google.android.gms.org.conscrypt.NativeCrypto.EVP_DigestSignFinal(Native method)
```

Reporter	[Deleted User]
Type	Bug
Priority	P2
Severity	S2
Status	Won't fix (Infeasible)
Access	Default access View
Assignee	ad...@google.com
Verifier	--
Collaborators	
CC	[Deleted User]
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

sart/runtime/check_jni.cc:65] at com.google.android.gms.org.conscrypt.OpenSSLSignature.engineSign(:com.google.android.gms@12874010@12.8.74 (020400-204998136):2)
sart/runtime/check_jni.cc:65] at java.security.Signature$SignatureImpl.engineSign(Signature.java:659)
sart/runtime/check_jni.cc:65] at java.security.Signature.sign(Signature.java:368)
sart/runtime/check_jni.cc:65] at com.android.org.bouncycastle.x509.X509Util.calculateSignature(X509Util.java:248)
sart/runtime/check_jni.cc:65] at com.android.org.bouncycastle.x509.X509V3CertificateGenerator.generate(X509V3CertificateGenerator.java:434)
sart/runtime/check_jni.cc:65] at com.android.org.bouncycastle.x509.X509V3CertificateGenerator.generate(X509V3CertificateGenerator.java:412)
sart/runtime/check_jni.cc:65] at android.security.AndroidKeyPairGenerator.generateKeyPair(AndroidKeyPairGenerator.java:133)
sart/runtime/check_jni.cc:65] at java.security.KeyPairGenerator$KeyPairGeneratorImpl.generateKeyPair(KeyPairGenerator.java:276)

Without the security provider updating key generation completes successfully on both Android versions.
When using RSA algorithm instead of EC, key generation again completes successfully.

I've attached sample code which can be called to reproduce the issue.

Any ideas? Has anyone faced such problem?
Thanks in advance.

updateSecurityProviderAndGenerateKeyPair.txt
2.1 KB View Download

COMMENTS

All comments ↓ Oldest first

ry...@gmail.com <ry...@gmail.com> #2 Oct 16, 2018 10:40PM

Hi,

We are facing the exact same issue regarding the ISE

java.lang.IllegalStateException: Can't generate certificate
at android.security.AndroidKeyPairGenerator.generateKeyPair(AndroidKeyPairGenerator.java:137)
at java.security.KeyPairGenerator$KeyPairGeneratorImpl.generateKeyPair(KeyPairGenerator.java:275)

Any update on a patch for this?

ad...@google.com <ad...@google.com> #3 Dec 13, 2018 10:21PM

Assigned to ad...@google.com.

Thank you for reporting this issue. For us to further investigate this issue, please provide the following additional information:

We are unable to check this issue with code given in comment #1.
Please provide sample project or apk to reproduce the issue. Also mention the steps to be followed for reproducing the issue with the given sample project or apk.

Frequency
How frequently does this issue occur? (e.g 100% of the time, 10% of the time)

Android build
Which Android build are you using? (e.g. KVT49L)

Device used
Which device did you use to reproduce this issue?

Are you able to reproduce the issue on Android Emulator & latest Android O & P on Pixel/Nexus devices ?

Android bug report
After reproducing the issue, press the volume up, volume down, and power button simultaneously. This will capture a bug report on your device in the “bug reports” directory. Attach the bug report file to this issue.

Alternate method:
After reproducing the issue, navigate to developer settings, ensure ‘USB debugging’ is enabled, then enable ‘Bug report shortcut’. To take bug report, hold the power button and select the ‘Take bug report’

option.

NOTE: Please upload the files to Google Drive and share the folder to android-bugreport@google.com, then share the link here.

ad...@google.com <ad...@google.com> #4 Dec 20, 2018 08:33PM

Please provide the information requested in comment #3 to investigate this issue further.

ad...@google.com <ad...@google.com> #5 Dec 27, 2018 09:24PM

Status: Won't Fix (Infeasible)

We are closing this issue as we don't have enough actionable information. If you are still facing this problem, please open new issue and add the relevant information along with reference to earlier issue.