Code signature

Table of Contents

1. About code signature

1.1 public key and private key

Public and private key:

http://www.ruanyifeng.com/blog/2013/06/rsa_algorithm_part_one.html
http://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

Case example:

Chinese version:

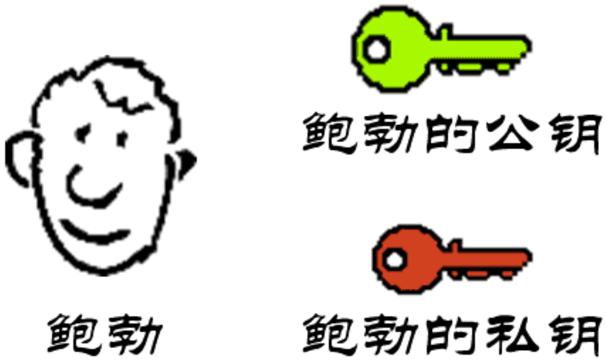
http://www.blogjava.net/yxhxj2006/archive/2012/10/15/389547.html

English version:

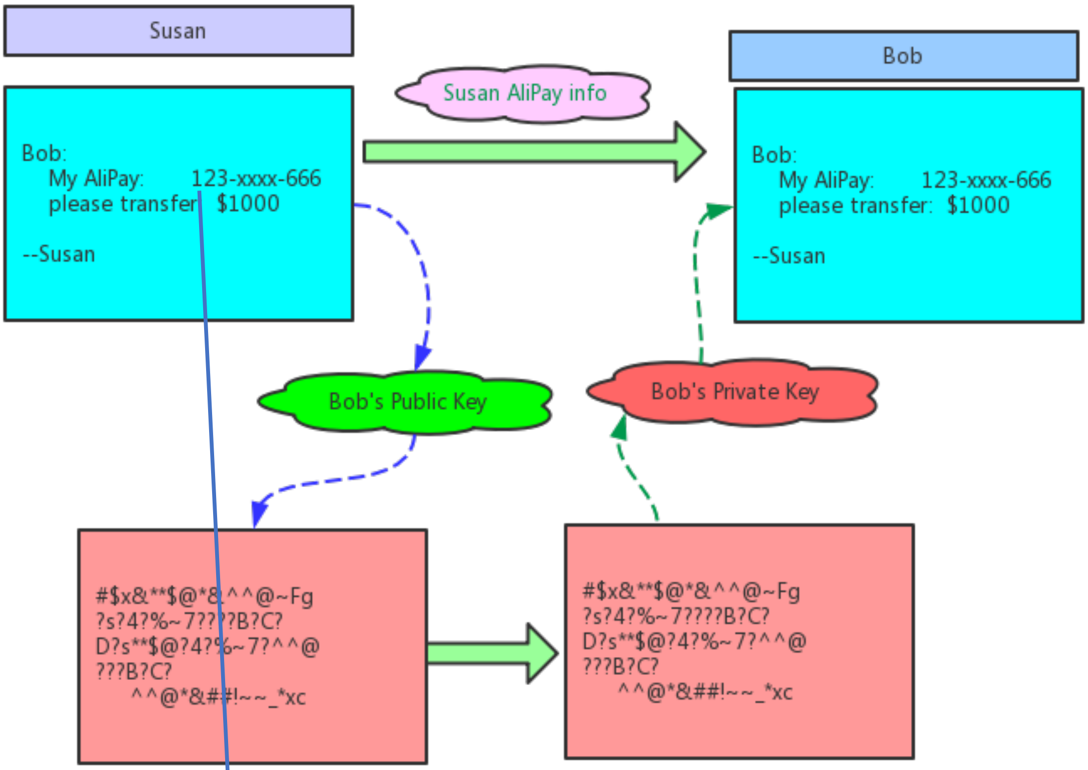
http://www.youdzone.com/signature.html

1.2 Common case

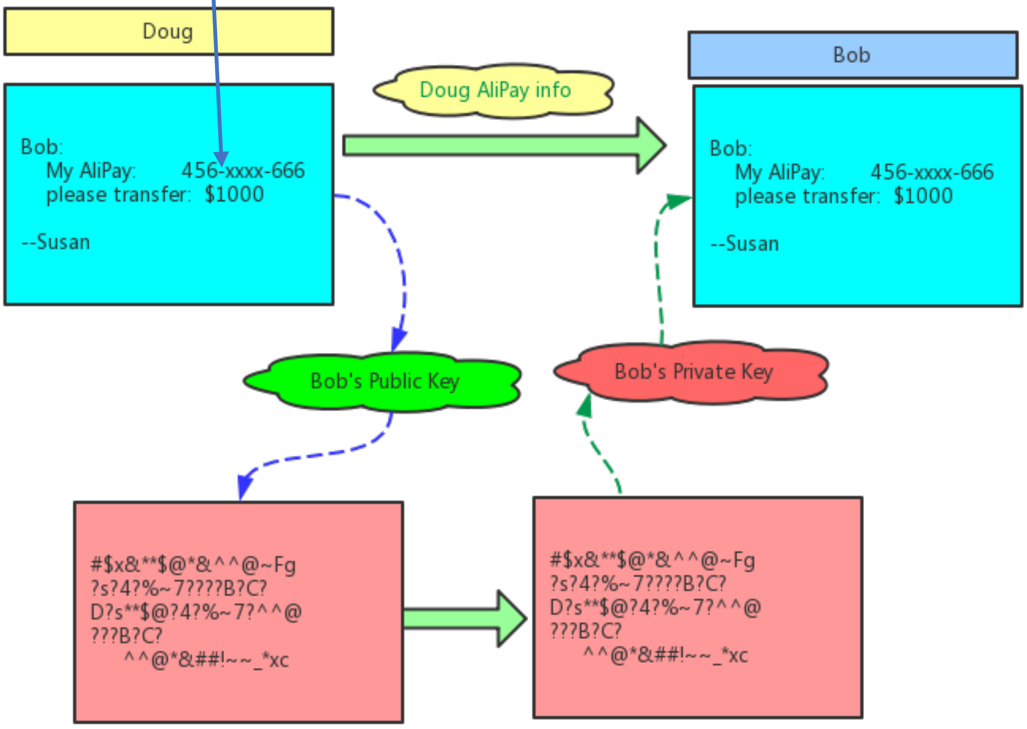
- **Bob: AliPay 777-xxxx-666**
- **Susan: AliPay 123-xxxx-666**
- **Doug: AliPay 456-xxxx-666**
- **Pat**



每人一把
帕蒂
道格
苏珊

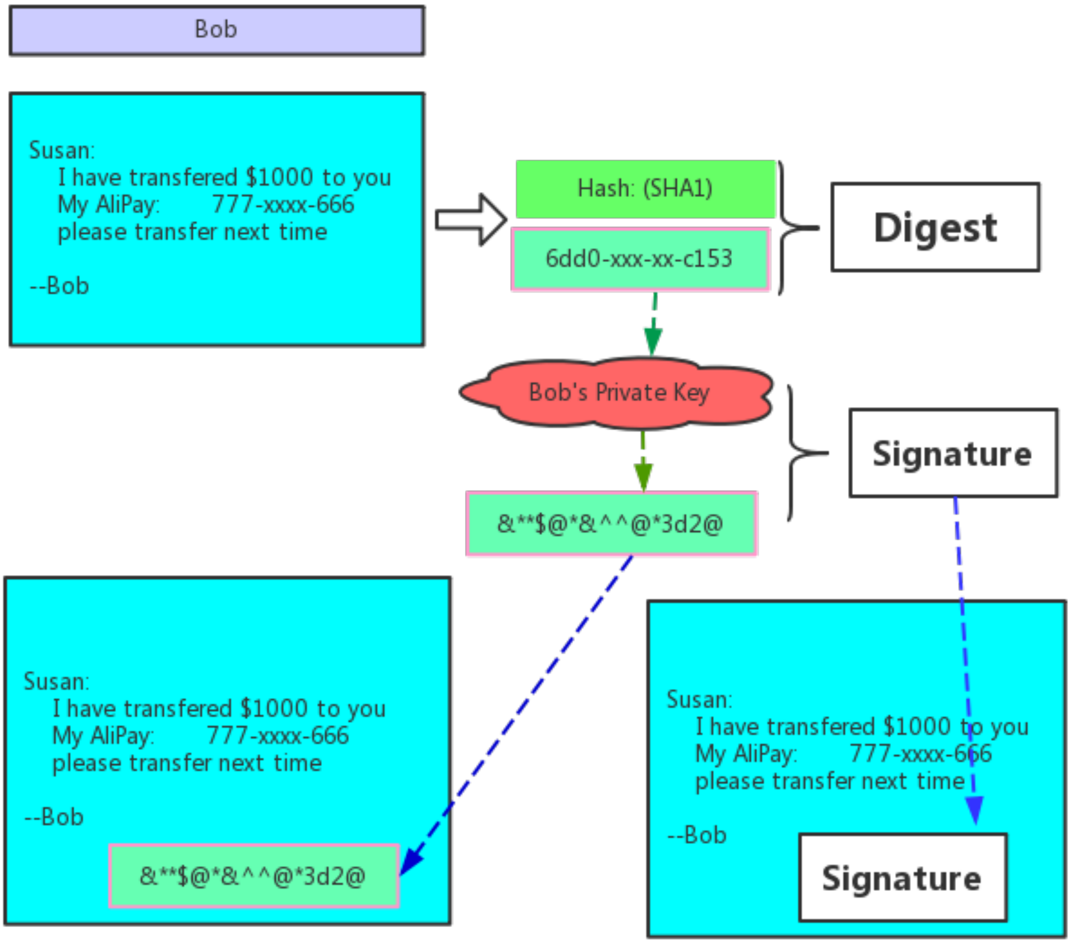


Doug also has Bob's public key, he wants to pretend to be Susan

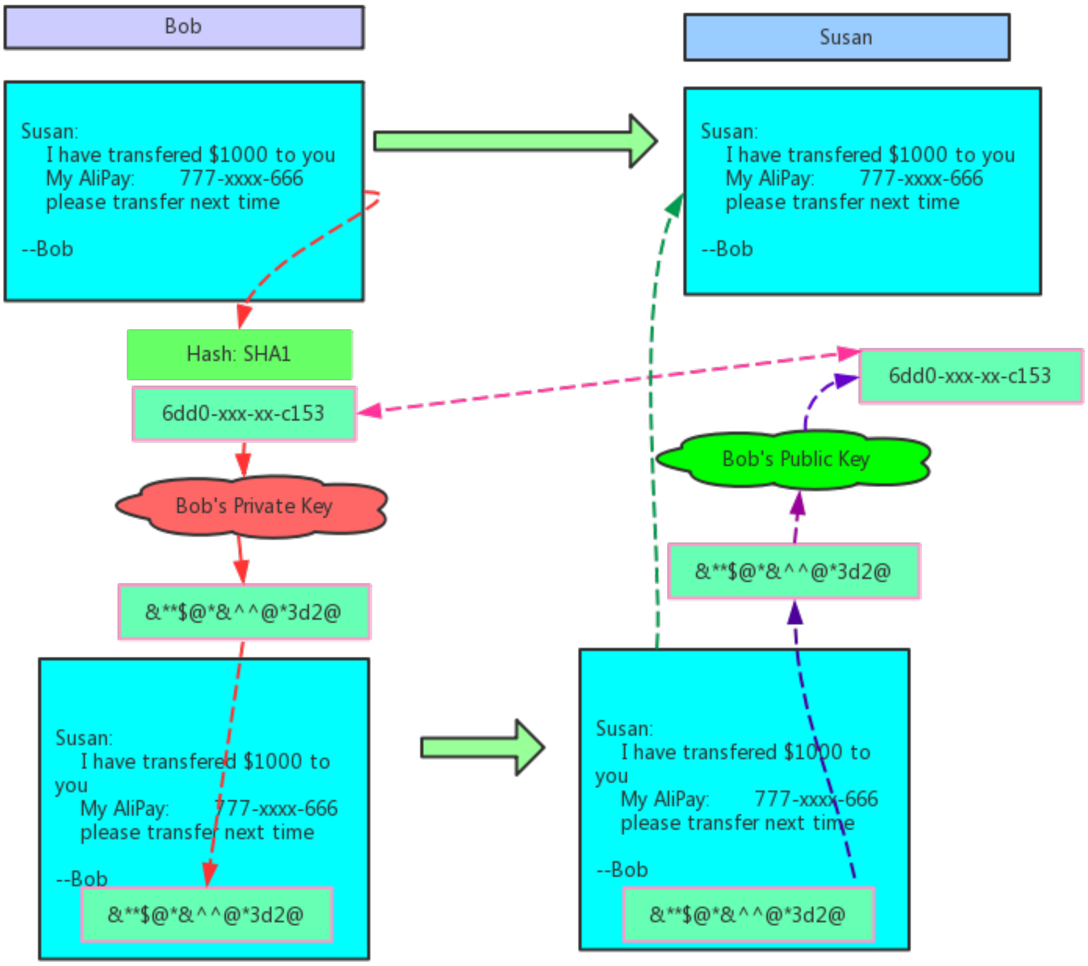


1.3 Digest and signature

basic concept about digest and signature

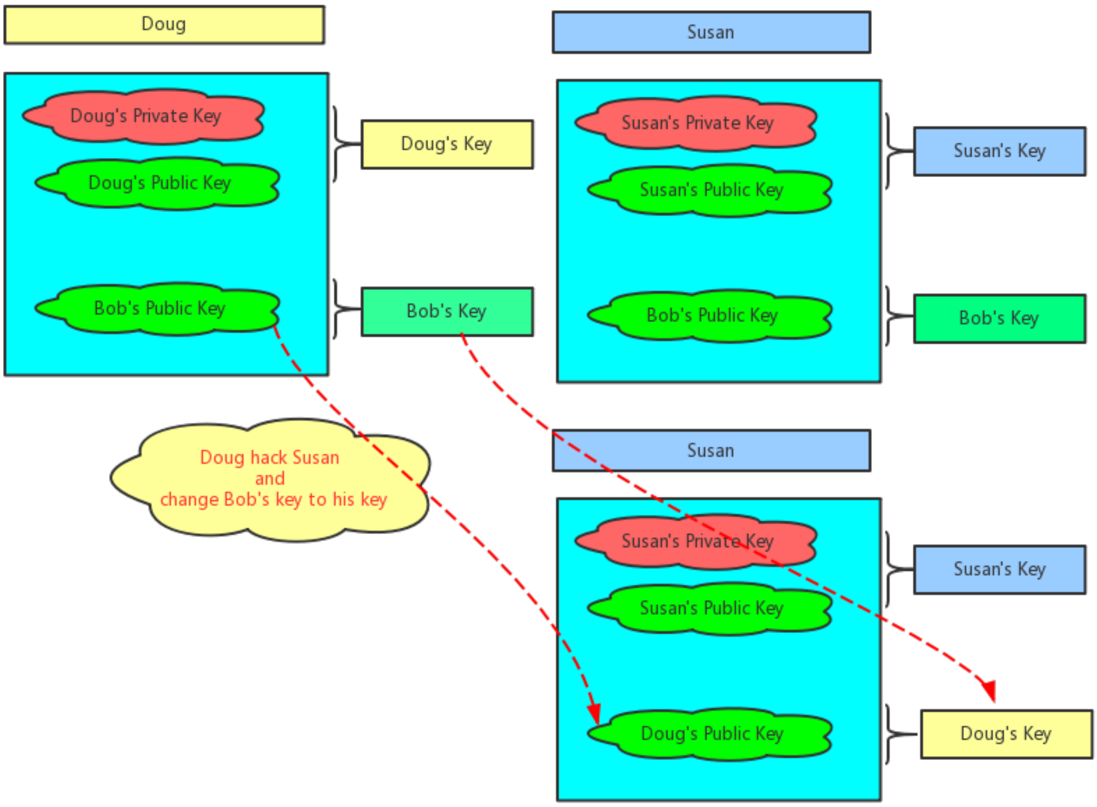


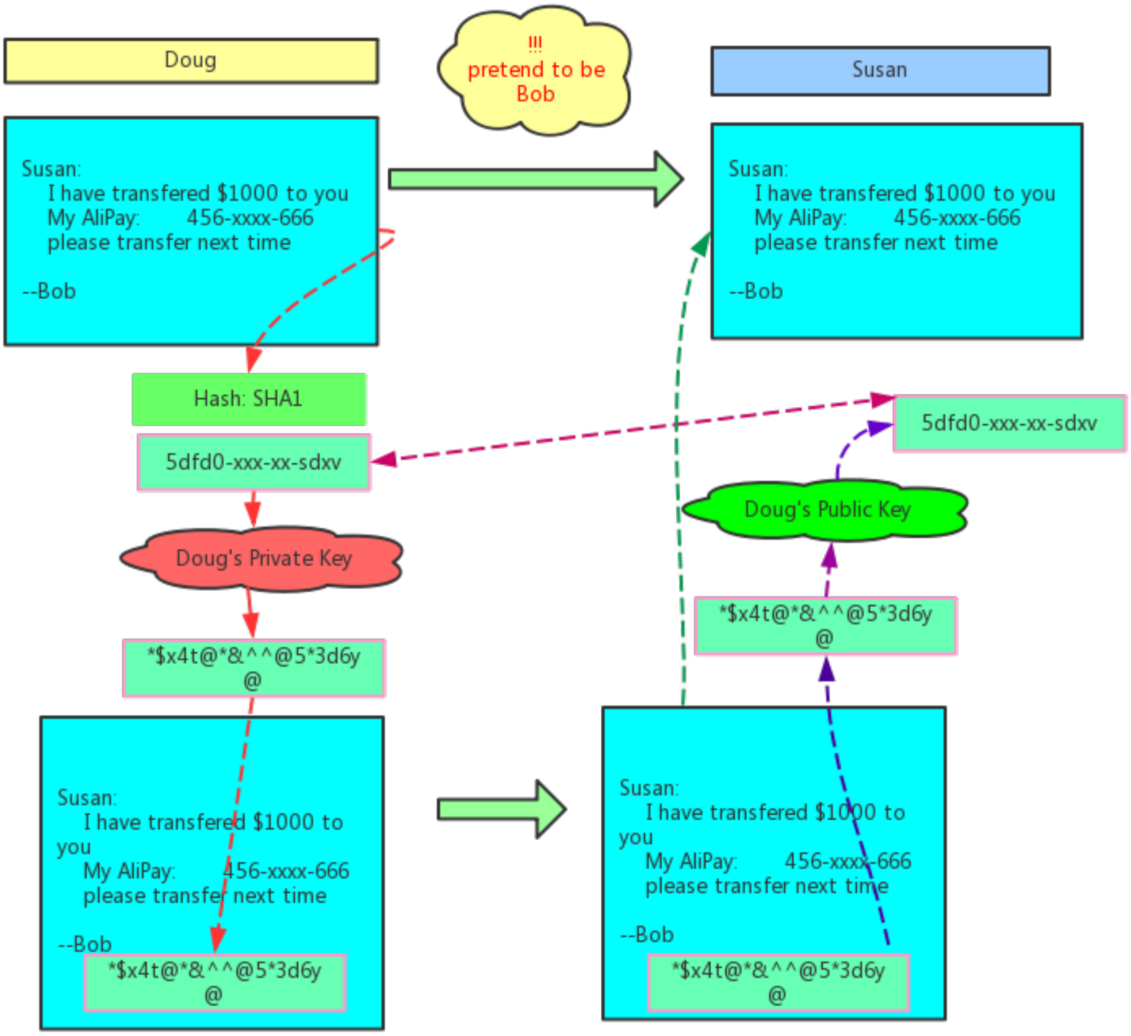
Common case for using digest and signature



Vulnerability :

case for using digest and signature





Doug

!!!
pretend to be
Bob

Susan

Susan:
I have transfered $1000 to you
My AliPay: 456-xxxx-666
please transfer next time

--Bob

Susan:
I have transfered $1000 to you
My AliPay: 456-xxxx-666
please transfer next time

--Bob

Hash: SHA1

5dfd0-xxx-xx-sdxv

5dfd0-xxx-xx-sdxv

Doug's Public Key

Doug's Private Key

$x4t@&^^@5*3d6y
@

$x4t@&^^@5*3d6y
@

Susan:
I have transfered $1000 to you
My AliPay: 456-xxxx-666
please transfer next time

--Bob

$x4t@&^^@5*3d6y
@

Susan:
I have transfered $1000 to you
My AliPay: 456-xxxx-666
please transfer next time

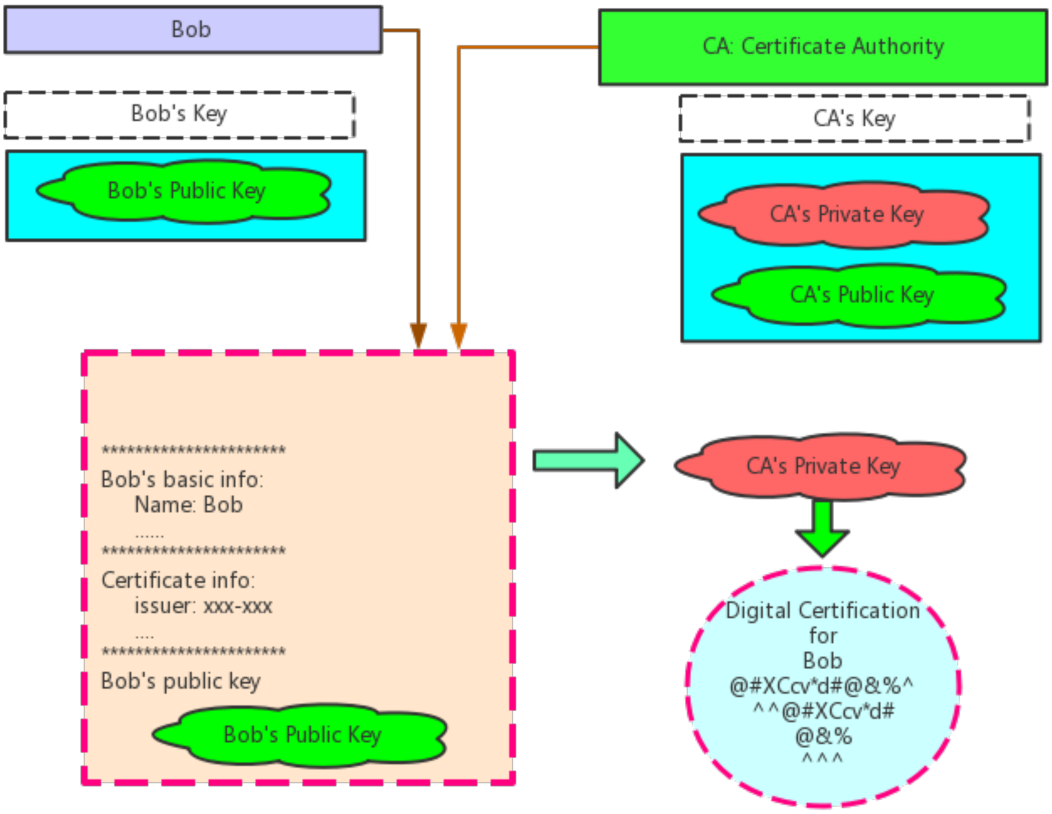
--Bob

$x4t@&^^@5*3d6y
@

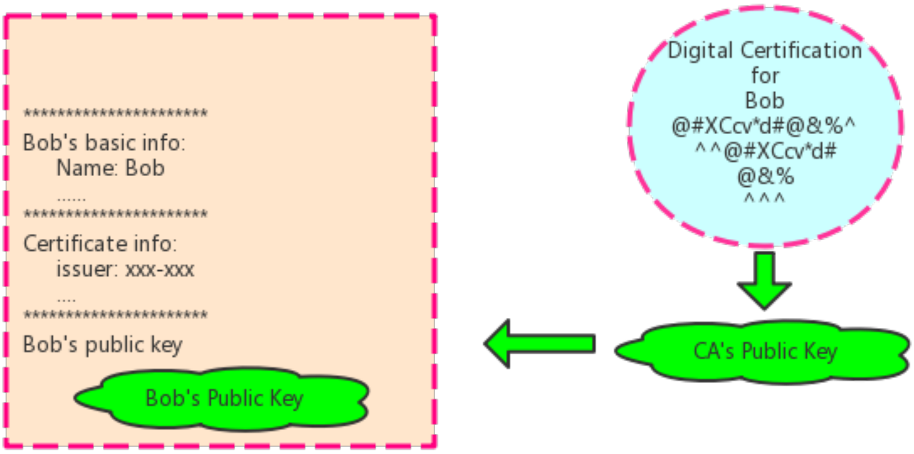
1.4 CA--certificate authority center and Digital certification

Susan not sure the public key is from Bob or from Doug.
So Susan does not trust the public key.
And she want to get this from CA center, which certificate that the Bob’s public key

CA generate certification for Bob based on Bob's public key

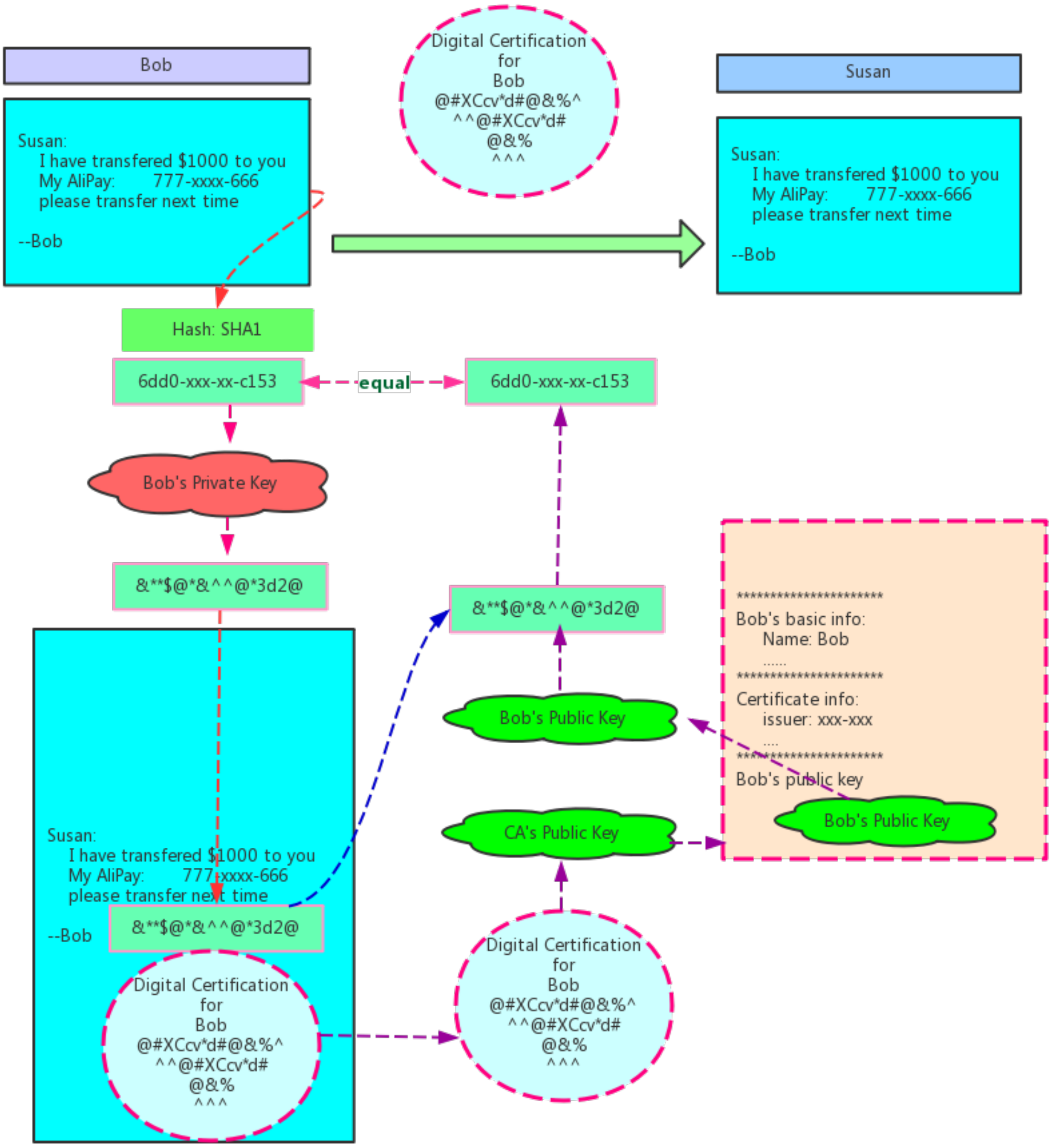


Get Bob's public key based on certification



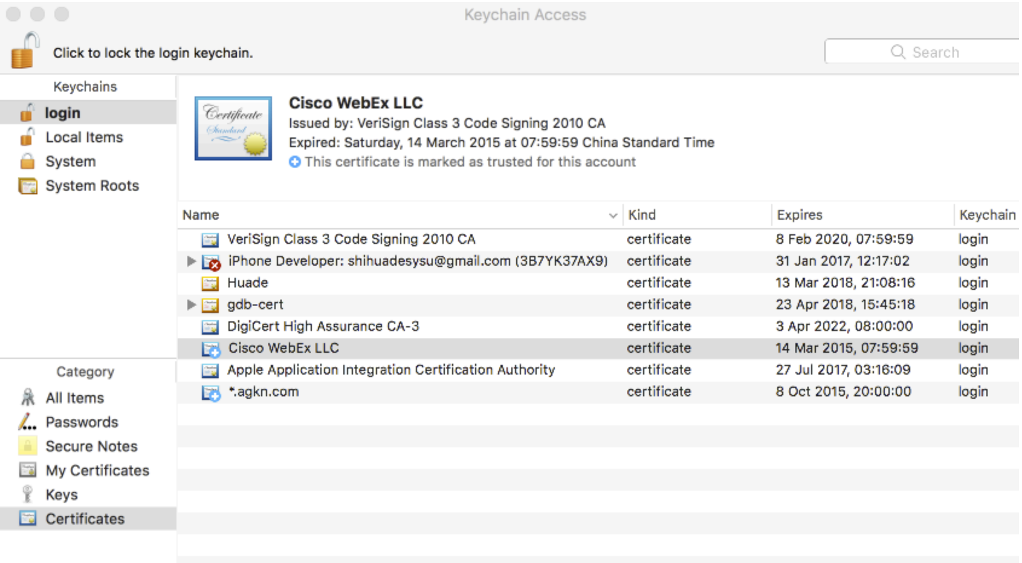
1.5 Communicate based on CA

Now Susan can verify that the Bob's public key did come from Bob
As it has been certificated by CA



1.6 Example for certification on Mac

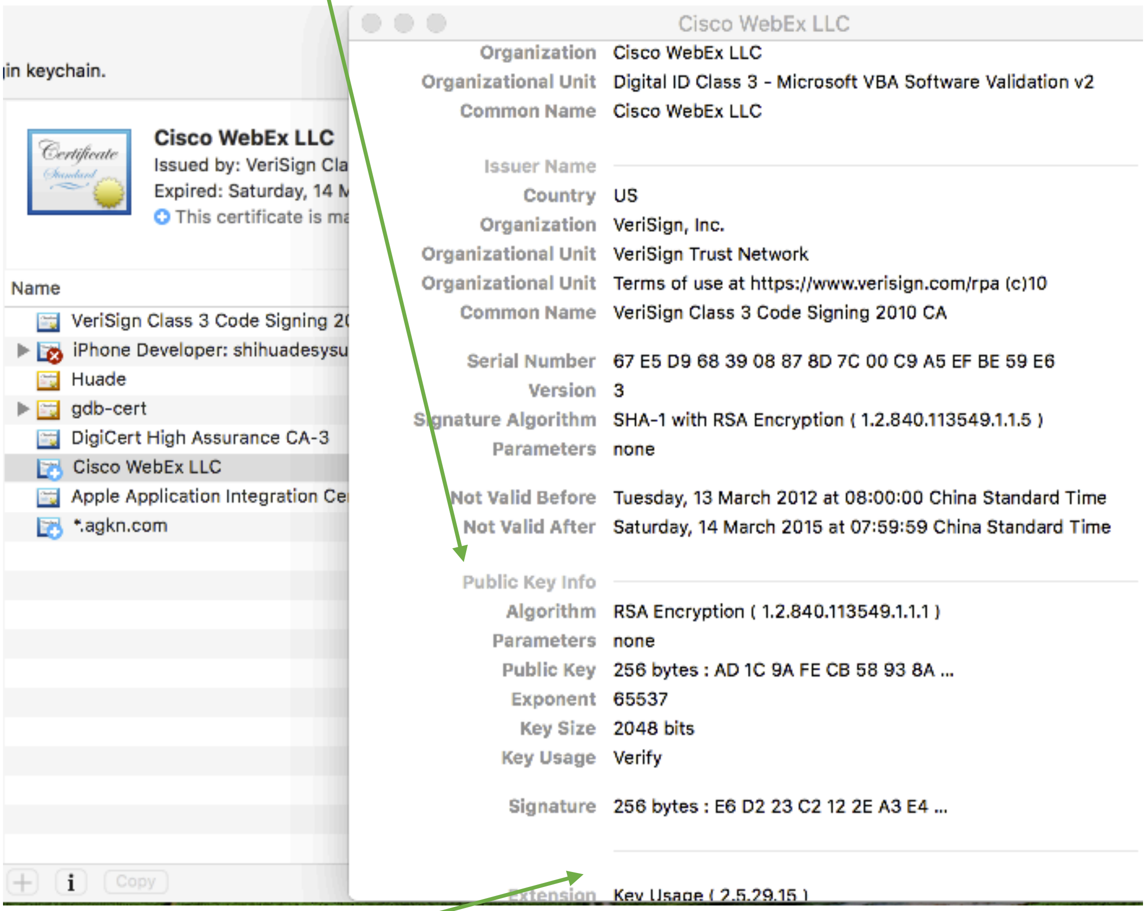
Go to keychain access



Cisco WebEx LLC
Issued by: VeriSign Class 3 Code Signing 2010 CA
Expired: Saturday, 14 March 2015 at 07:59:59 China Standard Time
This certificate is marked as trusted for this account

Name	Kind	Expires	Keychain
VeriSign Class 3 Code Signing 2010 CA	certificate	8 Feb 2020, 07:59:59	login
iPhone Developer: shihuadesysu@gmail.com (3B7YK37AX9)	certificate	31 Jan 2017, 12:17:02	login
Huade	certificate	13 Mar 2018, 21:08:16	login
gdb-cert	certificate	23 Apr 2018, 15:45:18	login
DigiCert High Assurance CA-3	certificate	3 Apr 2022, 08:00:00	login
Cisco WebEx LLC	certificate	14 Mar 2015, 07:59:59	login
Apple Application Integration Certification Authority	certificate	27 Jul 2017, 03:16:09	login
*.agkn.com	certificate	8 Oct 2015, 20:00:00	login

Public key info for Cisco WebEx LLC



Cisco WebEx LLC

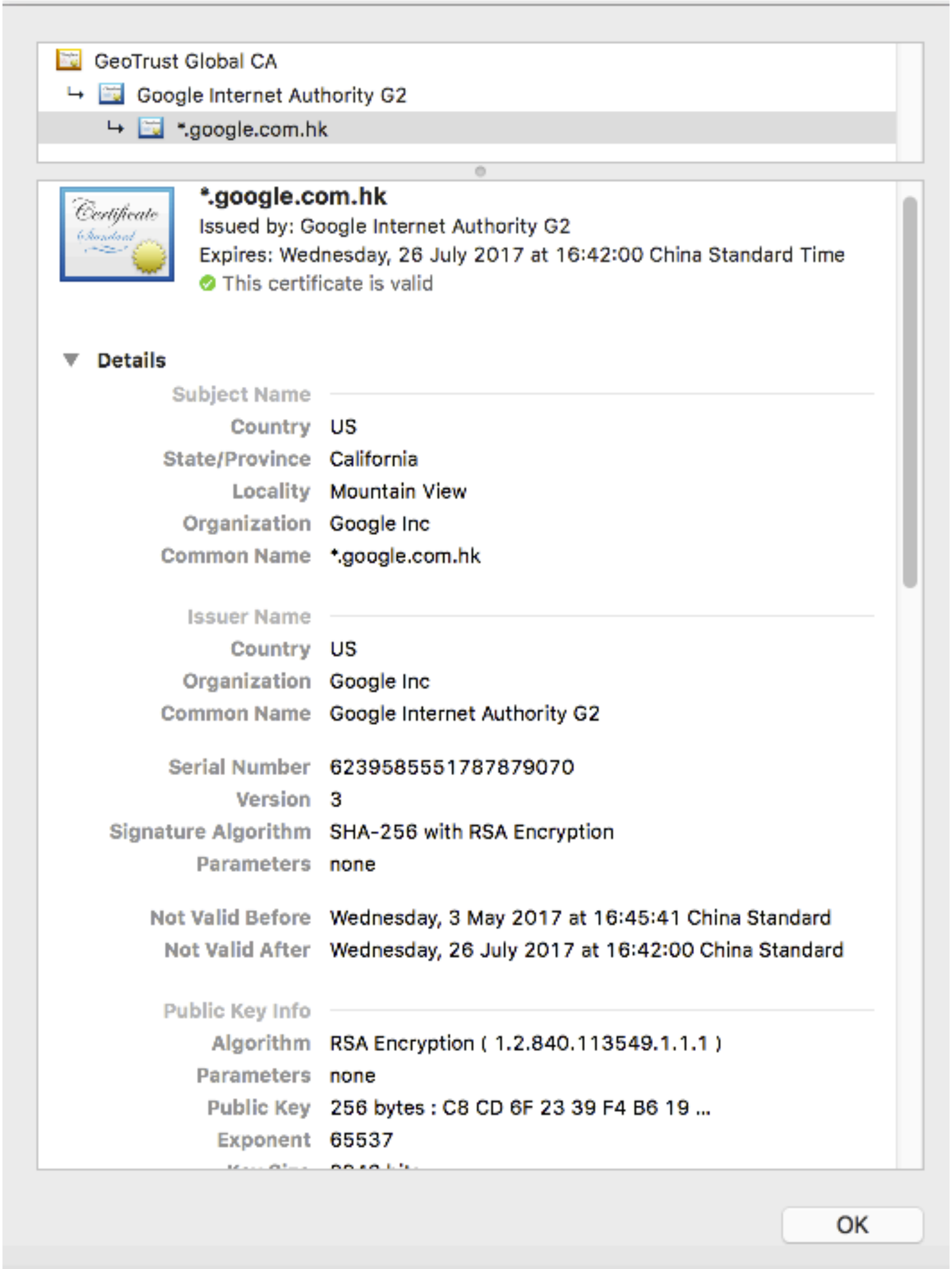
Organization	Cisco WebEx LLC
Organizational Unit	Digital ID Class 3 - Microsoft VBA Software Validation v2
Common Name	Cisco WebEx LLC
Issuer Name	
Country	US
Organization	VeriSign, Inc.
Organizational Unit	VeriSign Trust Network
Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Common Name	VeriSign Class 3 Code Signing 2010 CA
Serial Number	67 E5 D9 68 39 08 87 8D 7C 00 C9 A5 EF BE 59 E6
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Tuesday, 13 March 2012 at 08:00:00 China Standard Time
Not Valid After	Saturday, 14 March 2015 at 07:59:59 China Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : AD 1C 9A FE CB 58 93 8A ...
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : E6 D2 23 C2 12 2E A3 E4 ...
Extension	Key Usage (2.5.29.15)

Symantec’s CA for Cisco WebExLLC

https://www.symantec.com/about/legal/repository.jsp#rpa-ts

1.7 Example for certification on website

Google website:



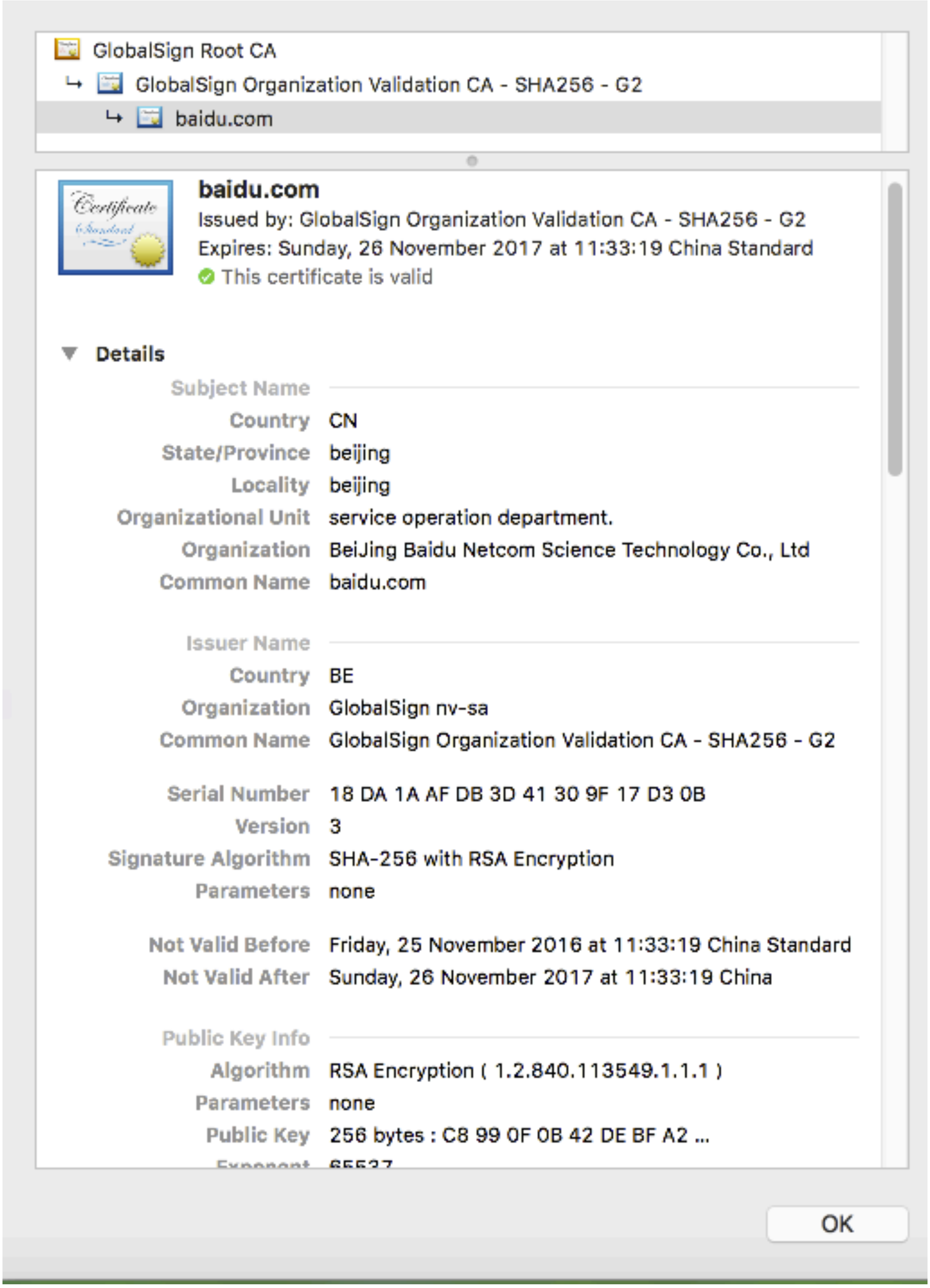
GeoTrust Global CA
↳ Google Internet Authority G2
↳ *.google.com.hk

***.google.com.hk**
Issued by: Google Internet Authority G2
Expires: Wednesday, 26 July 2017 at 16:42:00 China Standard Time
✓ This certificate is valid

▼ **Details**

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	*.google.com.hk
Issuer Name	
Country	US
Organization	Google Inc
Common Name	Google Internet Authority G2
Serial Number	6239585551787879070
Version	3
Signature Algorithm	SHA-256 with RSA Encryption
Parameters	none
Not Valid Before	Wednesday, 3 May 2017 at 16:45:41 China Standard
Not Valid After	Wednesday, 26 July 2017 at 16:42:00 China Standard
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : C8 CD 6F 23 39 F4 B6 19 ...
Exponent	65537

Baidu website:
Baidu's CA: https://www.globalsign.com/en/repository/



GlobalSign Root CA
↳ GlobalSign Organization Validation CA - SHA256 - G2
↳ baidu.com

baidu.com
Issued by: GlobalSign Organization Validation CA - SHA256 - G2
Expires: Sunday, 26 November 2017 at 11:33:19 China Standard
✓ This certificate is valid

▼ **Details**

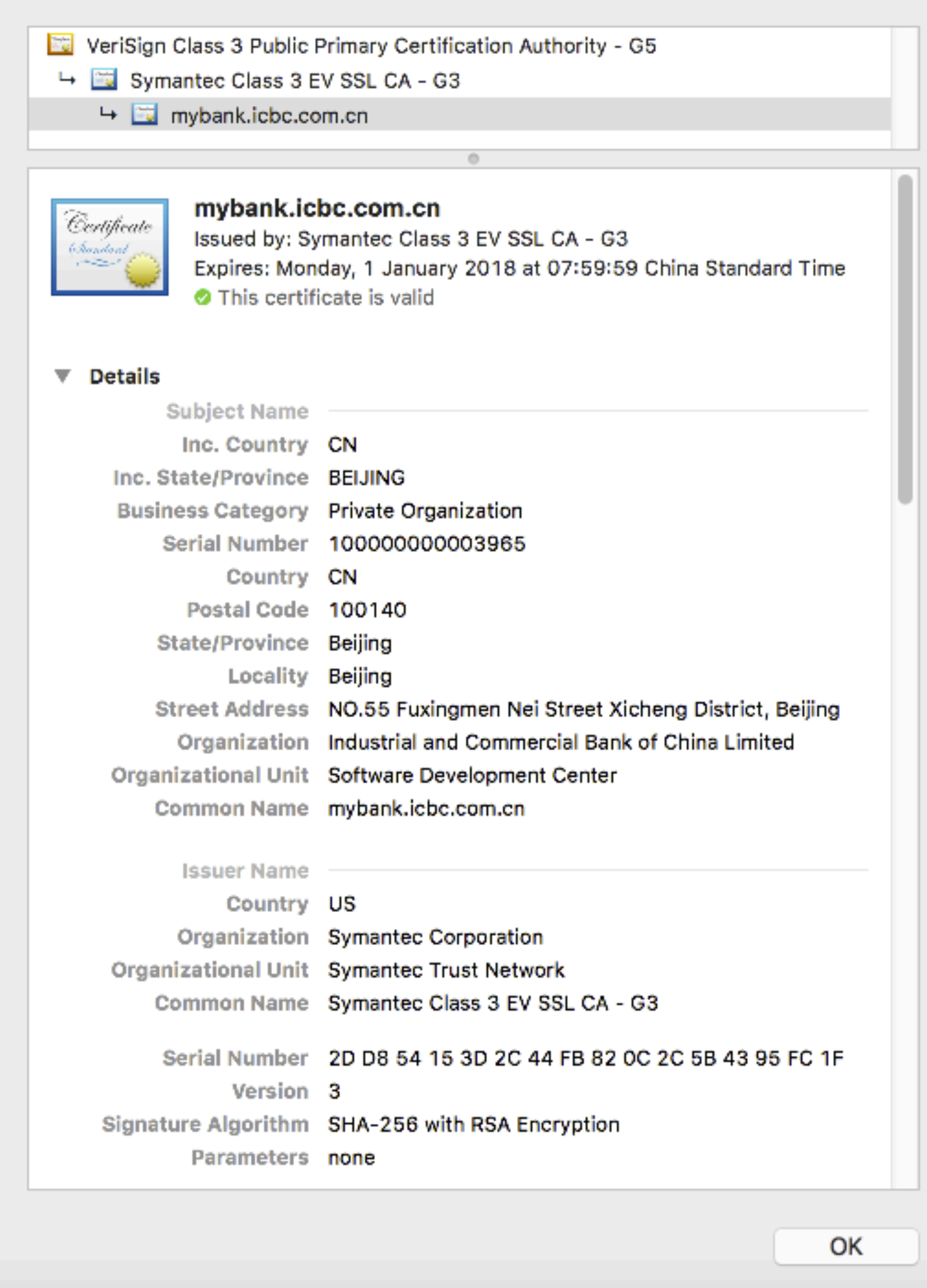
Subject Name	
Country	CN
State/Province	beijing
Locality	beijing
Organizational Unit	service operation department.
Organization	BeiJing Baidu Netcom Science Technology Co., Ltd
Common Name	baidu.com
Issuer Name	
Country	BE
Organization	GlobalSign nv-sa
Common Name	GlobalSign Organization Validation CA - SHA256 - G2
Serial Number	18 DA 1A AF DB 3D 41 30 9F 17 D3 0B
Version	3
Signature Algorithm	SHA-256 with RSA Encryption
Parameters	none
Not Valid Before	Friday, 25 November 2016 at 11:33:19 China Standard
Not Valid After	Sunday, 26 November 2017 at 11:33:19 China
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : C8 99 0F 0B 42 DE BF A2 ...
Exponent	65537

ICBC net bank

https://mybank.icbc.com.cn/icbc/newperbank/perbank3/frame/frame_index.jsp

CA by Symantec:

https://www.symantec.com/about/legal/repository.jsp#stn-cps



VeriSign Class 3 Public Primary Certification Authority - G5
↳ Symantec Class 3 EV SSL CA - G3
↳ mybank.icbc.com.cn

mybank.icbc.com.cn
Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Monday, 1 January 2018 at 07:59:59 China Standard Time
✓ This certificate is valid

▼ **Details**

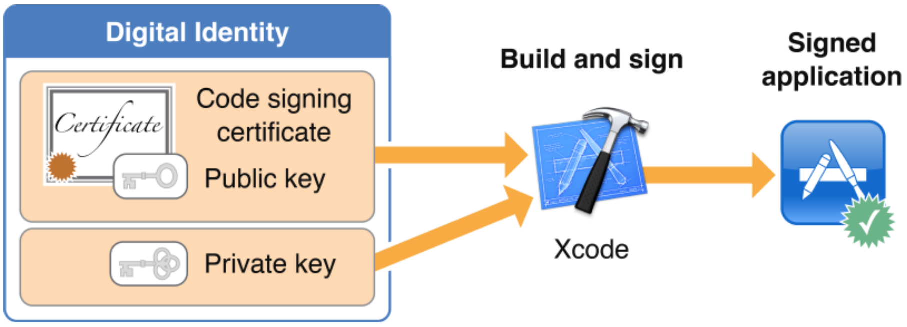
Subject Name	
Inc. Country	CN
Inc. State/Province	BEIJING
Business Category	Private Organization
Serial Number	100000000003965
Country	CN
Postal Code	100140
State/Province	Beijing
Locality	Beijing
Street Address	NO.55 Fuxingmen Nei Street Xicheng District, Beijing
Organization	Industrial and Commercial Bank of China Limited
Organizational Unit	Software Development Center
Common Name	mybank.icbc.com.cn
Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	Symantec Trust Network
Common Name	Symantec Class 3 EV SSL CA - G3
Serial Number	2D D8 54 15 3D 2C 44 FB 82 0C 2C 5B 43 95 FC 1F
Version	3
Signature Algorithm	SHA-256 with RSA Encryption
Parameters	none

2. Example certification for ios/mac developer

2.1 example

Application Code Signing

https://developer.apple.com/library/content/documentation/General/Conceptual/DevPedia-CocoaCore/AppSigning.html

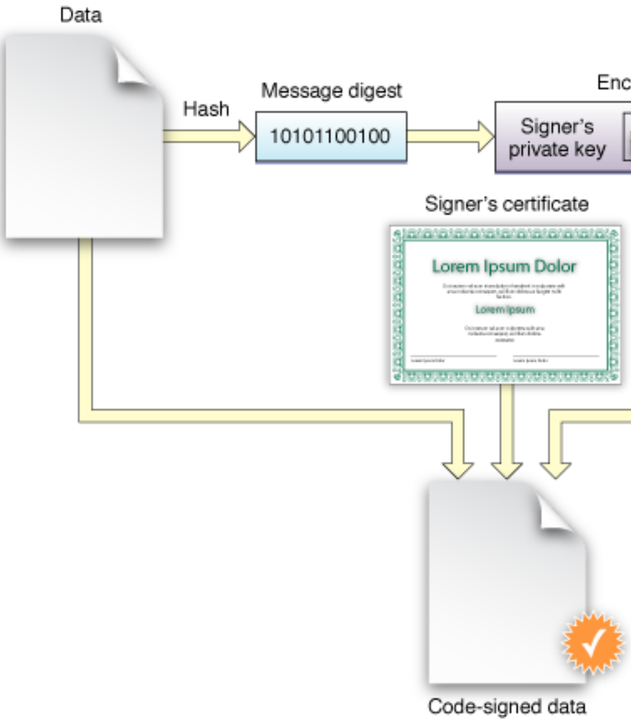


Example in Chinese:

http://foggry.com/blog/2014/10/16/ios-code-signing-xue-xi-bi-ji/

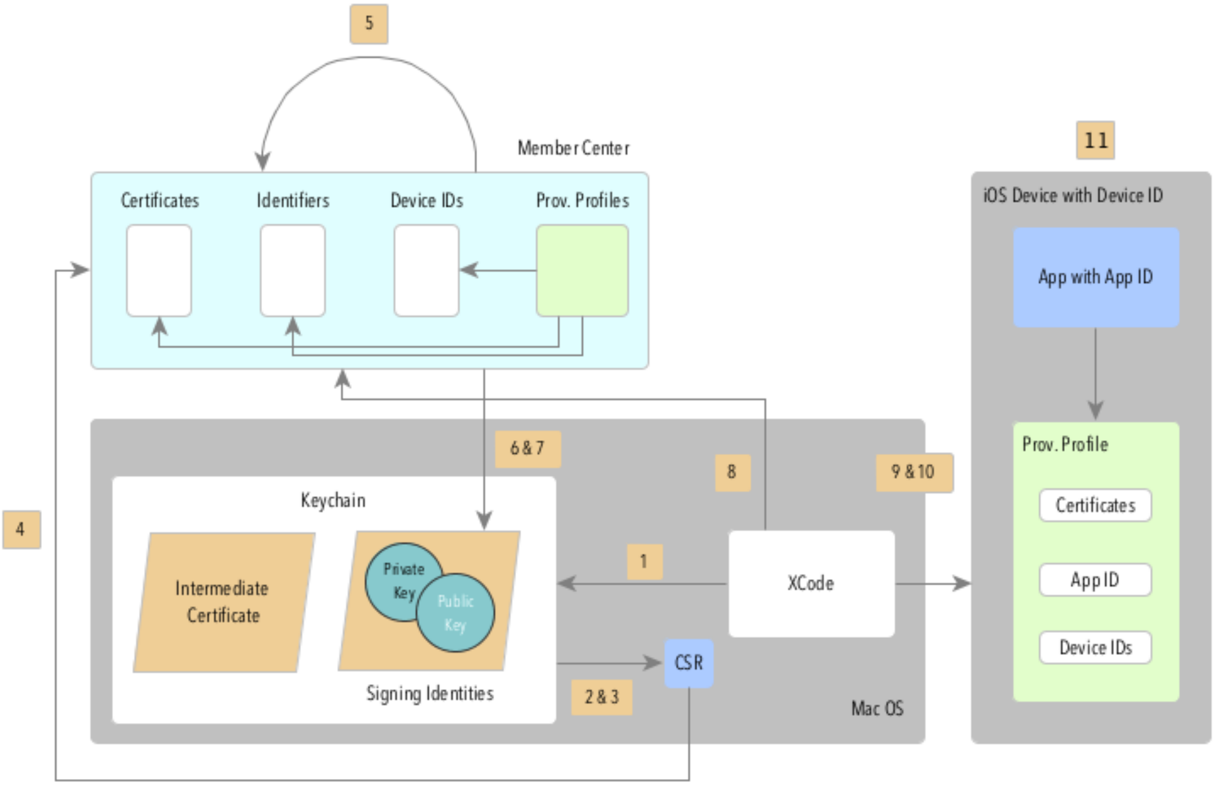
Code signature for mac

http://osxdaily.com/2016/03/14/verify-code-sign-apps-mac-os-x/



Example for iOS Code Signing & Provisioning in a Nutshell

https://medium.com/ios-os-x-development/ios-code-signing-provisioning-in-a-nutshell-d5b247760bef



3. How to verify code signature

3.1 verifycation for Mac app

Example website:

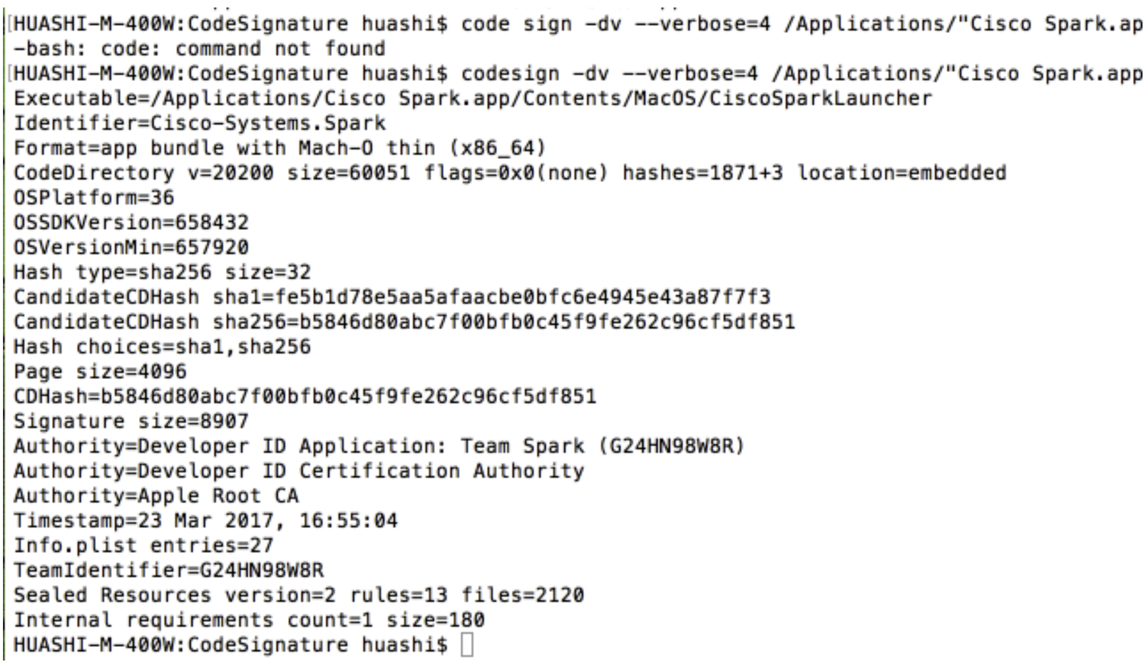
http://osxdaily.com/2016/03/14/verify-code-sign-apps-mac-os-x/

Command:

```
codesign -dv --verbose=4  /Path/To/Application.app
```

Verification for Spark app:

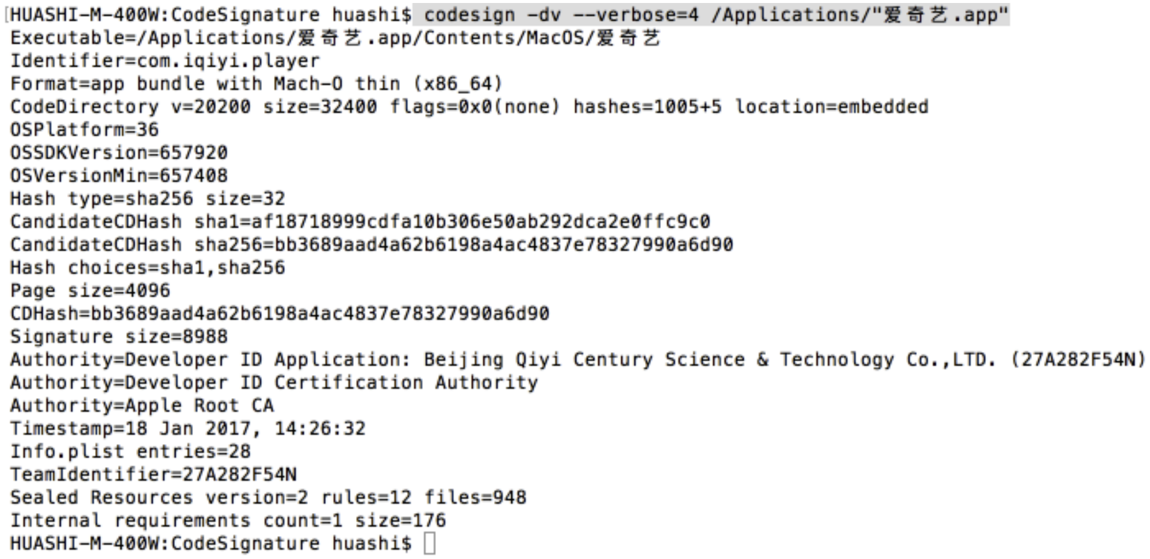
```
codesign -dv --verbose=4 /Applications/"Cisco Spark.app"
```



```
HUASHI-M-400W:CodeSignature huashi$ code sign -dv --verbose=4 /Applications/"Cisco Spark.ap
-bash: code: command not found
HUASHI-M-400W:CodeSignature huashi$ codesign -dv --verbose=4 /Applications/"Cisco Spark.app
Executable=/Applications/Cisco Spark.app/Contents/MacOS/CiscoSparkLauncher
Identifier=Cisco-Systems.Spark
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20200 size=60051 flags=0x0(none) hashes=1871+3 location=embedded
OSPlatform=36
OSSDKVersion=658432
OSVersionMin=657920
Hash type=sha256 size=32
CandidateCDHash sha1=fe5b1d78e5aa5afaacbe0bfc6e4945e43a87f7f3
CandidateCDHash sha256=b5846d80abc7f00bfb0c45f9fe262c96cf5df851
Hash choices=sha1,sha256
Page size=4096
CDHash=b5846d80abc7f00bfb0c45f9fe262c96cf5df851
Signature size=8907
Authority=Developer ID Application: Team Spark (G24HN98W8R)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=23 Mar 2017, 16:55:04
Info.plist entries=27
TeamIdentifier=G24HN98W8R
Sealed Resources version=2 rules=13 files=2120
Internal requirements count=1 size=180
HUASHI-M-400W:CodeSignature huashi$
```

Verification for 爱奇艺. app:

codesign -dv --verbose=4 /Applications/"爱奇艺.app"



```
[HUASHI-M-400W:CodeSignature huashi$ codesign -dv --verbose=4 /Applications/"爱奇艺.app"
Executable=/Applications/爱奇艺.app/Contents/MacOS/爱奇艺
Identifier=com.iqiyi.player
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20200 size=32400 flags=0x0(none) hashes=1005+5 location=embedded
OSPlatform=36
OSSDKVersion=657920
OSVersionMin=657408
Hash type=sha256 size=32
CandidateCDHash sha1=af18718999cdfa10b306e50ab292dca2e0ffc9c0
CandidateCDHash sha256=bb3689aad4a62b6198a4ac4837e78327990a6d90
Hash choices=sha1,sha256
Page size=4096
CDHash=bb3689aad4a62b6198a4ac4837e78327990a6d90
Signature size=8988
Authority=Developer ID Application: Beijing Qiyi Century Science & Technology Co.,LTD. (27A282F54N)
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Timestamp=18 Jan 2017, 14:26:32
Info.plist entries=28
TeamIdentifier=27A282F54N
Sealed Resources version=2 rules=12 files=948
Internal requirements count=1 size=176
HUASHI-M-400W:CodeSignature huashi$ 
```

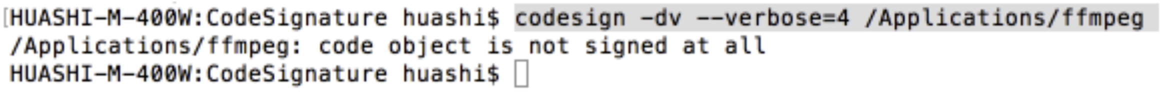
Verification for FFMPEG:

codesign -dv --verbose=4 /Applications/ffmpeg

ffmpeg is clone from:

`git://source.ffmpeg.org/ffmpeg.git`

and make install only without code signature



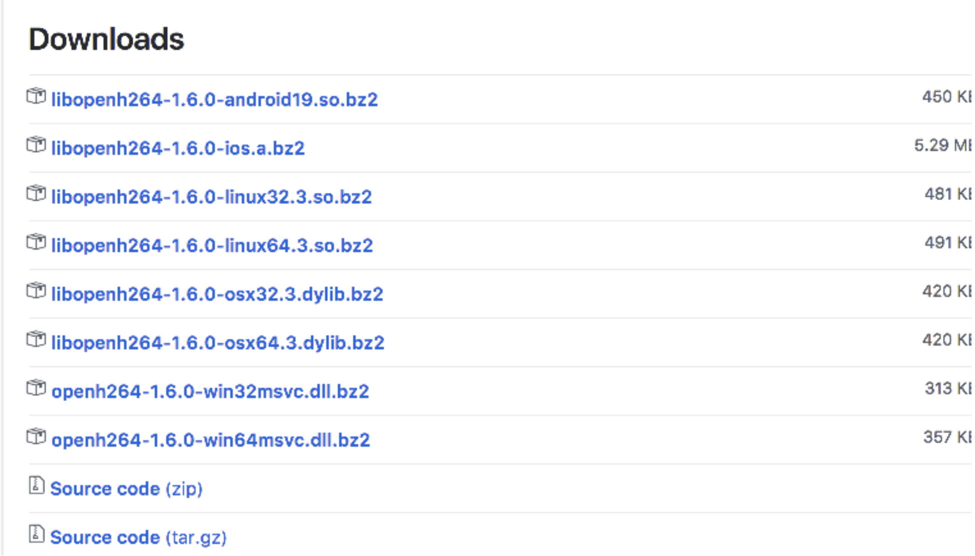
```
[HUASHI-M-400W:CodeSignature huashi$ codesign -dv --verbose=4 /Applications/ffmpeg
/Applications/ffmpeg: code object is not signed at all
HUASHI-M-400W:CodeSignature huashi$ 
```

3.2 verifycation for Mac dylib

Example for openh264 dylib code signature verification

Example for those code-signed packages from openh264 office website

Openh264 release package:
https://github.com/cisco/openh264/releases

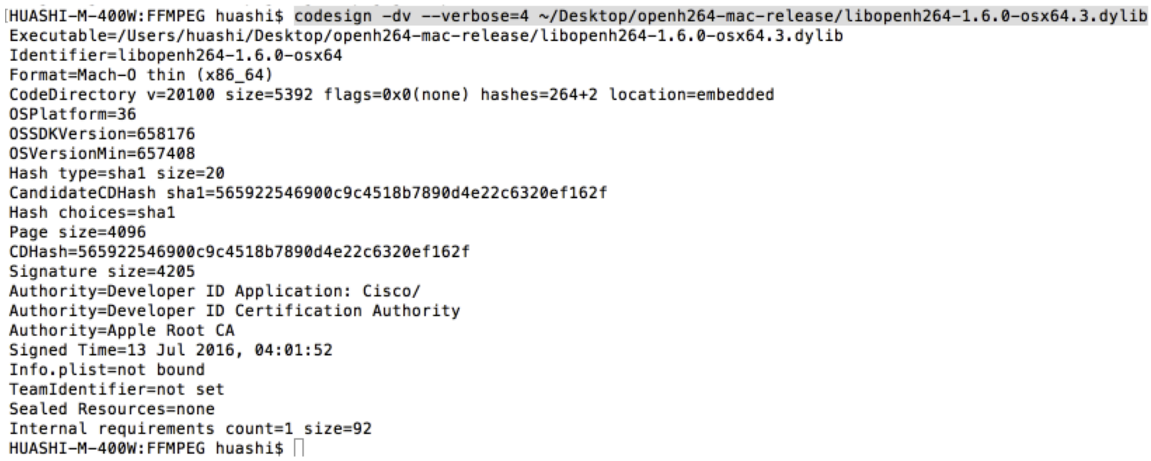


Downloads

libopenh264-1.6.0-android19.so.bz2	450 KI
libopenh264-1.6.0-ios.a.bz2	5.29 MI
libopenh264-1.6.0-linux32.3.so.bz2	481 KI
libopenh264-1.6.0-linux64.3.so.bz2	491 KI
libopenh264-1.6.0-osx32.3.dylib.bz2	420 KI
libopenh264-1.6.0-osx64.3.dylib.bz2	420 KI
openh264-1.6.0-win32msvc.dll.bz2	313 KI
openh264-1.6.0-win64msvc.dll.bz2	357 KI
Source code (zip)	
Source code (tar.gz)	

take libopenh264-1.6.0-osx64.3.dylib.bz2 for example:

```
codesign -dv --verbose=4 ~/Desktop/openh264-mac-release/libopenh264-1.6.0-osx64.3.dylib
```



```
HUASHI-M-400W:FFMPEG huashi$ codesign -dv --verbose=4 ~/Desktop/openh264-mac-release/libopenh264-1.6.0-osx64.3.dylib
Executable=/Users/huashi/Desktop/openh264-mac-release/libopenh264-1.6.0-osx64.3.dylib
Identifier=libopenh264-1.6.0-osx64
Format=Mach-O thin (x86_64)
CodeDirectory v=20100 size=5392 flags=0x0(none) hashes=264+2 location=embedded
OSPlatform=36
OSSDKVersion=658176
OSVersionMin=657408
Hash type=sha1 size=20
CandidateCDHash sha1=565922546900c9c4518b7890d4e22c6320ef162f
Hash choices=sha1
Page size=4096
CDHash=565922546900c9c4518b7890d4e22c6320ef162f
Signature size=4205
Authority=Developer ID Application: Cisco/
Authority=Developer ID Certification Authority
Authority=Apple Root CA
Signed Time=13 Jul 2016, 04:01:52
Info.plist=not bound
TeamIdentifier=not set
Sealed Resources=none
Internal requirements count=1 size=92
HUASHI-M-400W:FFMPEG huashi$ 
```

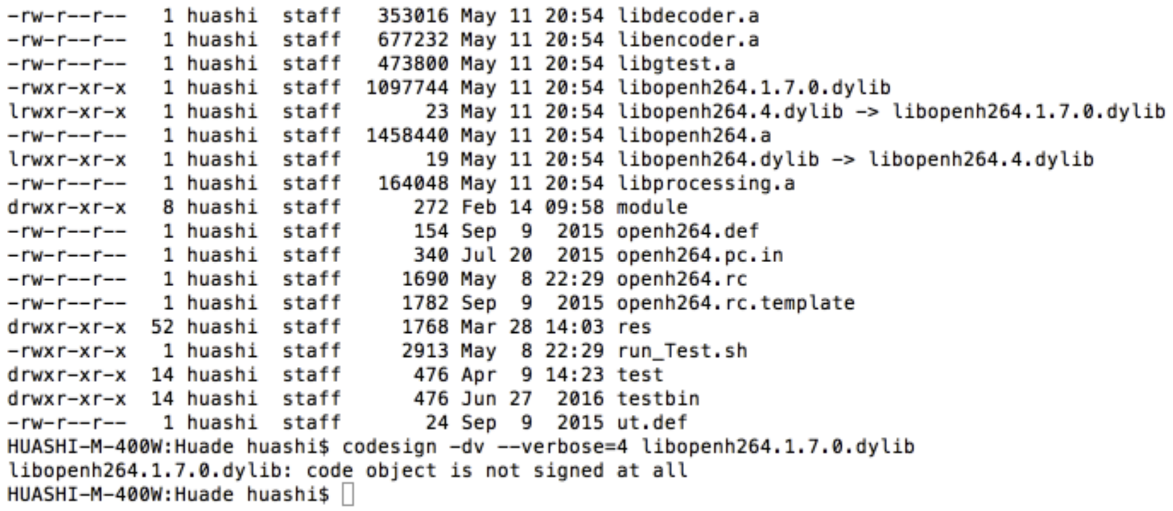
Example for make only without code signature

Clone openh264 from openh264 office website

https://github.com/cisco/openh264.git

and build dylib with command:

make



```
-rw-r--r--   1 huashi  staff   353016 May 11 20:54 libdecoder.a
-rw-r--r--   1 huashi  staff   677232 May 11 20:54 libencoder.a
-rw-r--r--   1 huashi  staff   473800 May 11 20:54 libgtest.a
-rwxr-xr-x   1 huashi  staff  1097744 May 11 20:54 libopenh264.1.7.0.dylib
lrwxr-xr-x   1 huashi  staff       23 May 11 20:54 libopenh264.4.dylib -> libopenh264.1.7.0.dylib
-rw-r--r--   1 huashi  staff  1458440 May 11 20:54 libopenh264.a
lrwxr-xr-x   1 huashi  staff       19 May 11 20:54 libopenh264.dylib -> libopenh264.4.dylib
-rw-r--r--   1 huashi  staff   164048 May 11 20:54 libprocessing.a
drwxr-xr-x   8 huashi  staff      272 Feb 14 09:58 module
-rw-r--r--   1 huashi  staff      154 Sep  9  2015 openh264.def
-rw-r--r--   1 huashi  staff      340 Jul 20  2015 openh264.pc.in
-rw-r--r--   1 huashi  staff     1690 May  8 22:29 openh264.rc
-rw-r--r--   1 huashi  staff     1782 Sep  9  2015 openh264.rc.template
drwxr-xr-x  52 huashi  staff     1768 Mar 28 14:03 res
-rwxr-xr-x   1 huashi  staff     2913 May  8 22:29 run_Test.sh
drwxr-xr-x  14 huashi  staff      476 Apr  9 14:23 test
drwxr-xr-x  14 huashi  staff      476 Jun 27  2016 testbin
-rw-r--r--   1 huashi  staff       24 Sep  9  2015 ut.def
HUASHI-M-400W:Huade huashi$ codesign -dv --verbose=4 libopenh264.1.7.0.dylib
libopenh264.1.7.0.dylib: code object is not signed at all
HUASHI-M-400W:Huade huashi$ 
```

4. Encrypt and decrypt

For how to encrypt/decrypt data/files/packages, please refer to:

https://gist.github.com/colinstein/de1755d2d7fbe27a0f1e

5. How to signature code

For how to signature code on different os, like ios/android/windows/mac/linux etc. You can get tool via google etc.

6. Website for reference

Mac

https://www.symantec.com/content/en/us/about/media/repository/root-certificates.pdf
http://osxdaily.com/2016/03/14/verify-code-sign-apps-mac-os-x/
https://www.digicert.com/code-signing/mac-os-codesign-tool.htm
http://osxdaily.com/2016/03/14/verify-code-sign-apps-mac-os-x/
https://developer.apple.com/library/content/documentation/Security/Conceptual/CodeSigningGuide/Procedures/Procedures.html

https://developer.apple.com/library/content/technotes/tn2206/_index.html

https://support.apple.com/en-us/HT202369

http://blog.leanote.com/post/yinhaide/MAC%E7%8E%AF%E5%A2%83%E4%B8%8B%E7%94%9F%E6%88%90Apple%E8%AF%81%E4%B9%A6%E6%95%99%E7%A8%8B

widows:

https://msdn.microsoft.com/en-us/library/ms537362(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/ms537361(v=vs.85).aspx

ios:

http://foggry.com/blog/2014/10/16/ios-code-signing-xue-xi-bi-ji/