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:

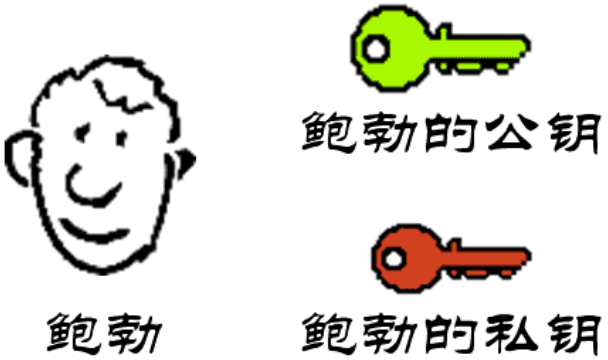
http://www.blogjava.net/yxhxj2006/archive/2012/10/15/389547.html

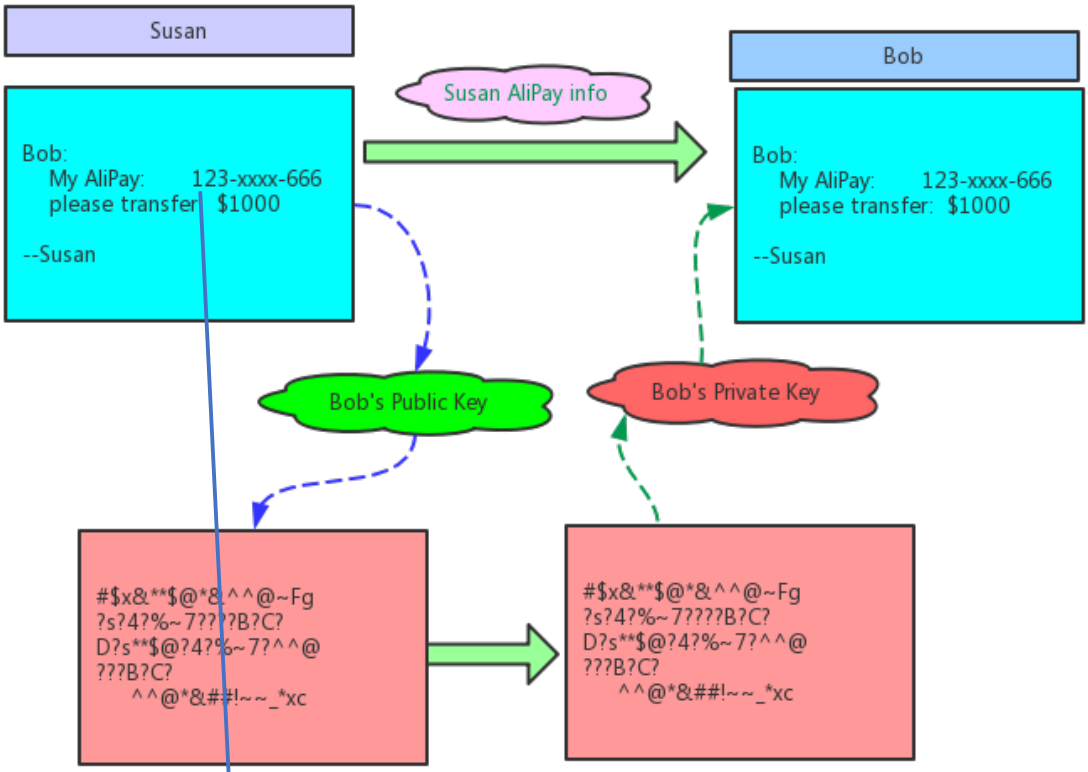
English version:

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

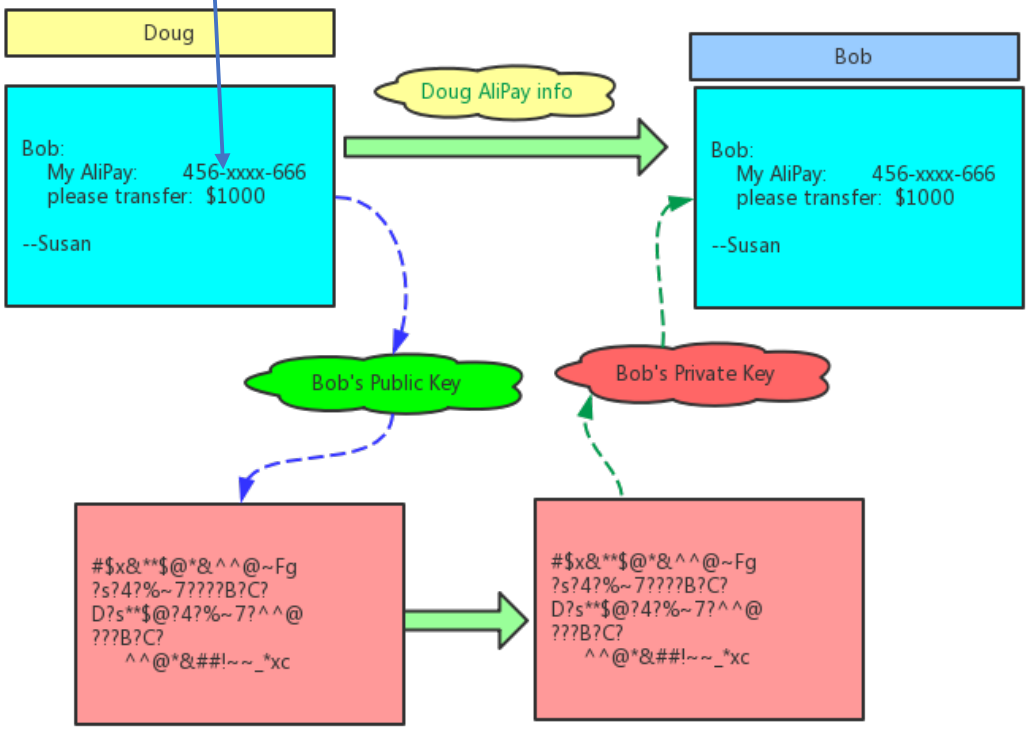
1.2 Common case

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



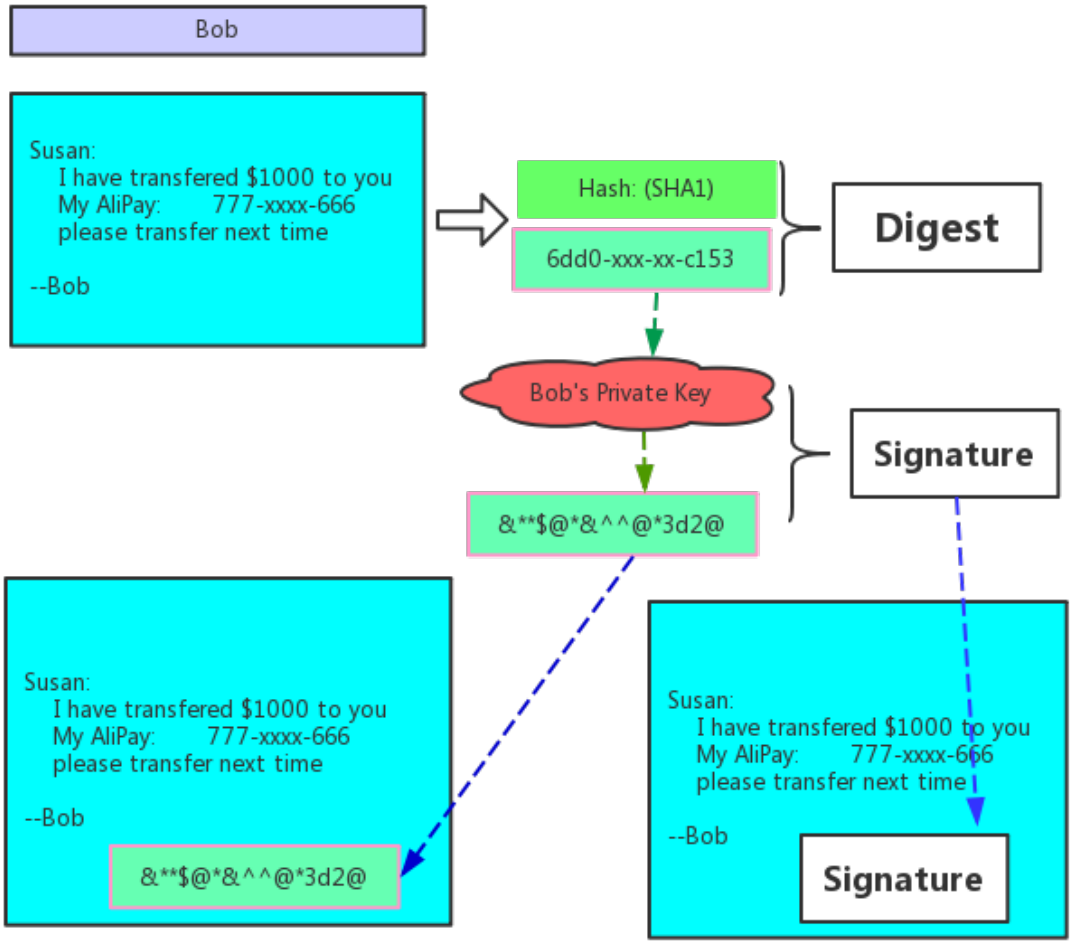


Doug also has Bob's public key, he wants to pretend to be Susan

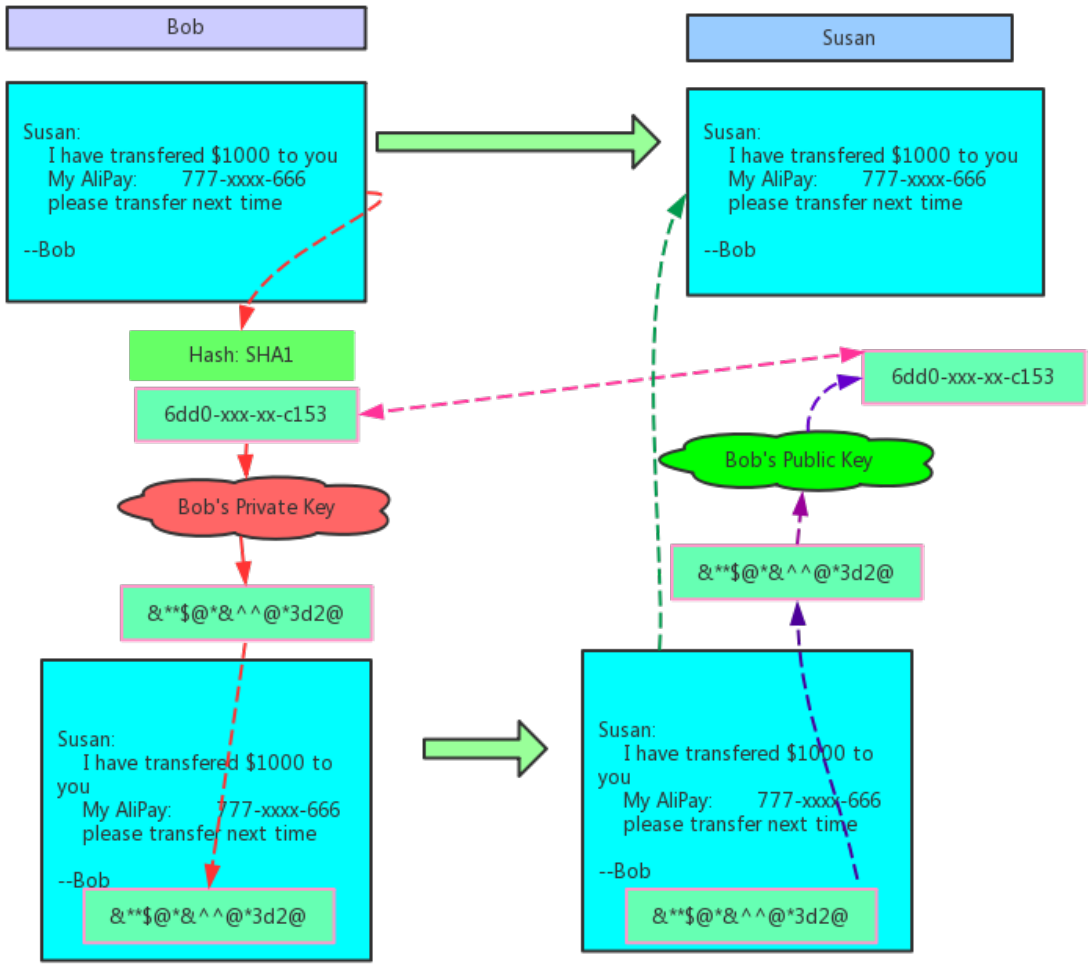


1.3 Digest and signature

basic concept about digest and signature

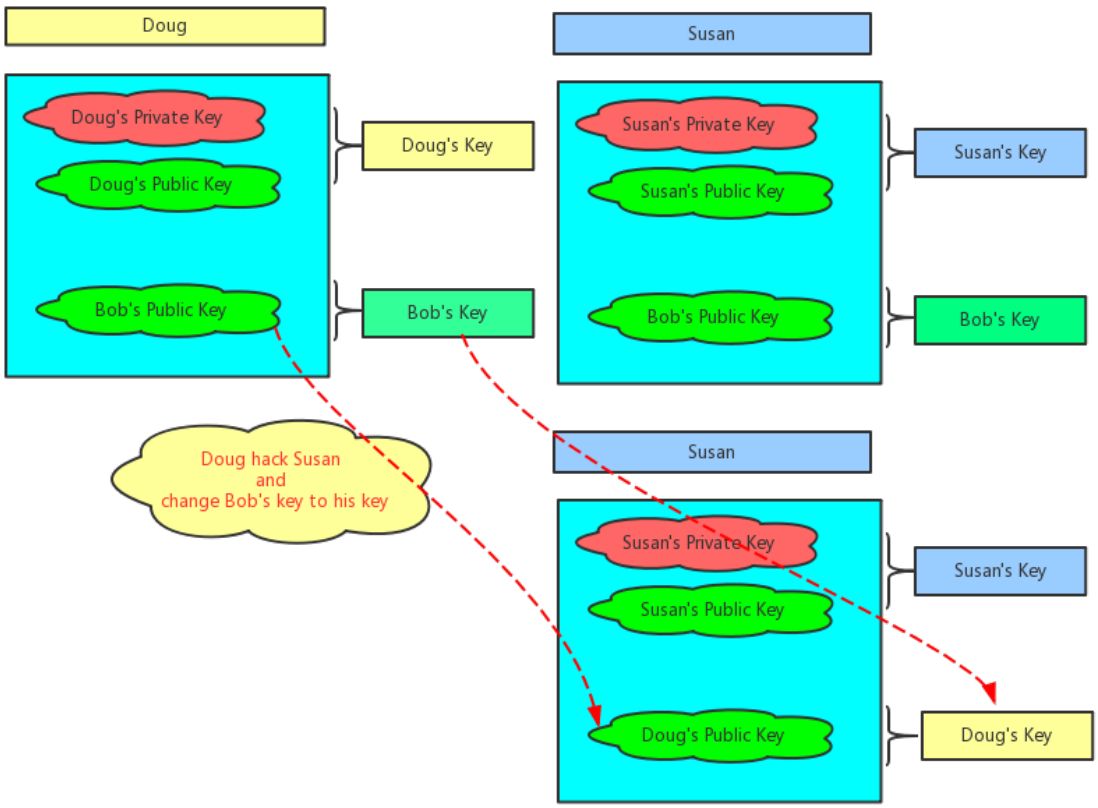


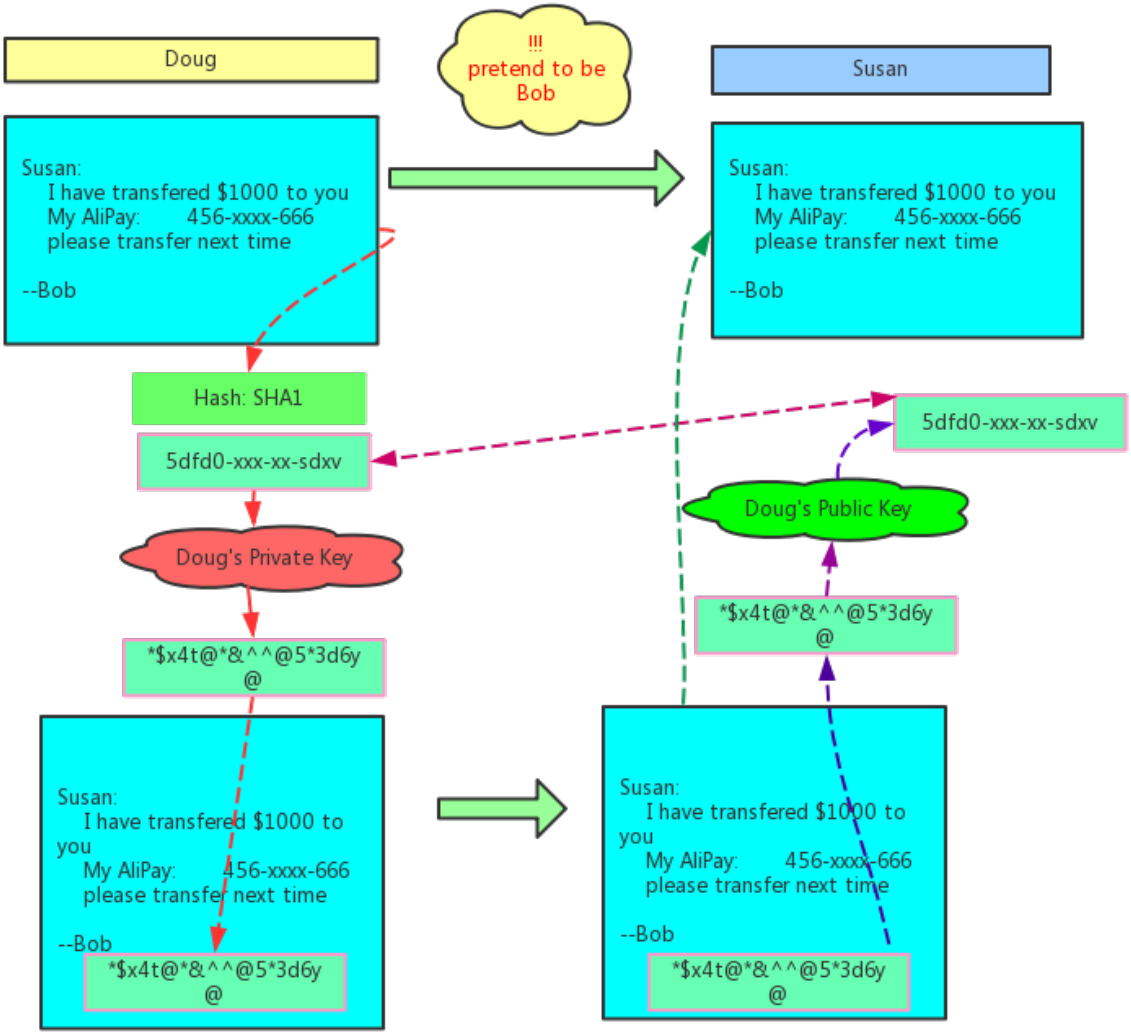
Common case for using digest and signature



Vulnerability：

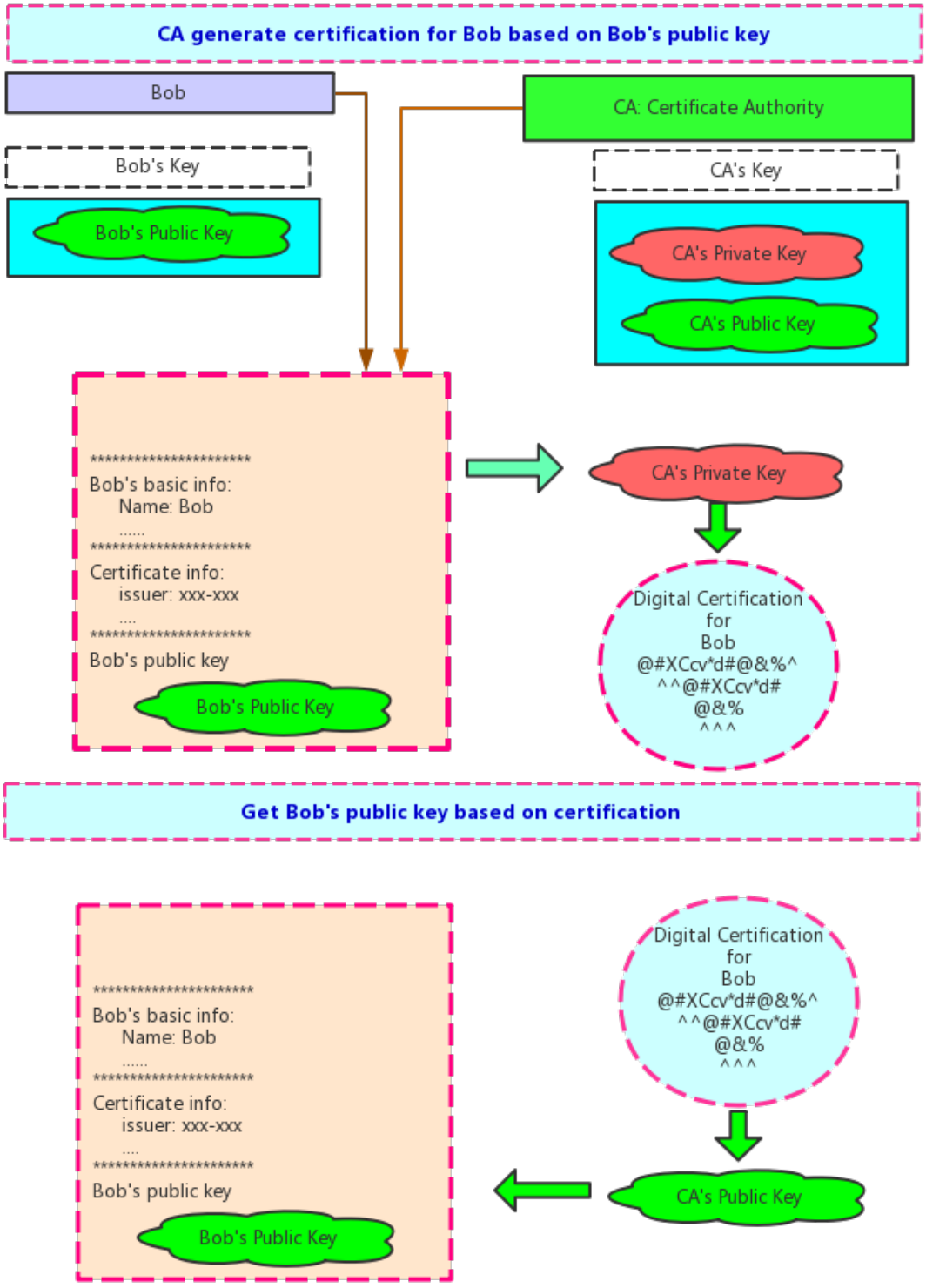
case for using digest and signature




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 Private Key
Doug's Public 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
@

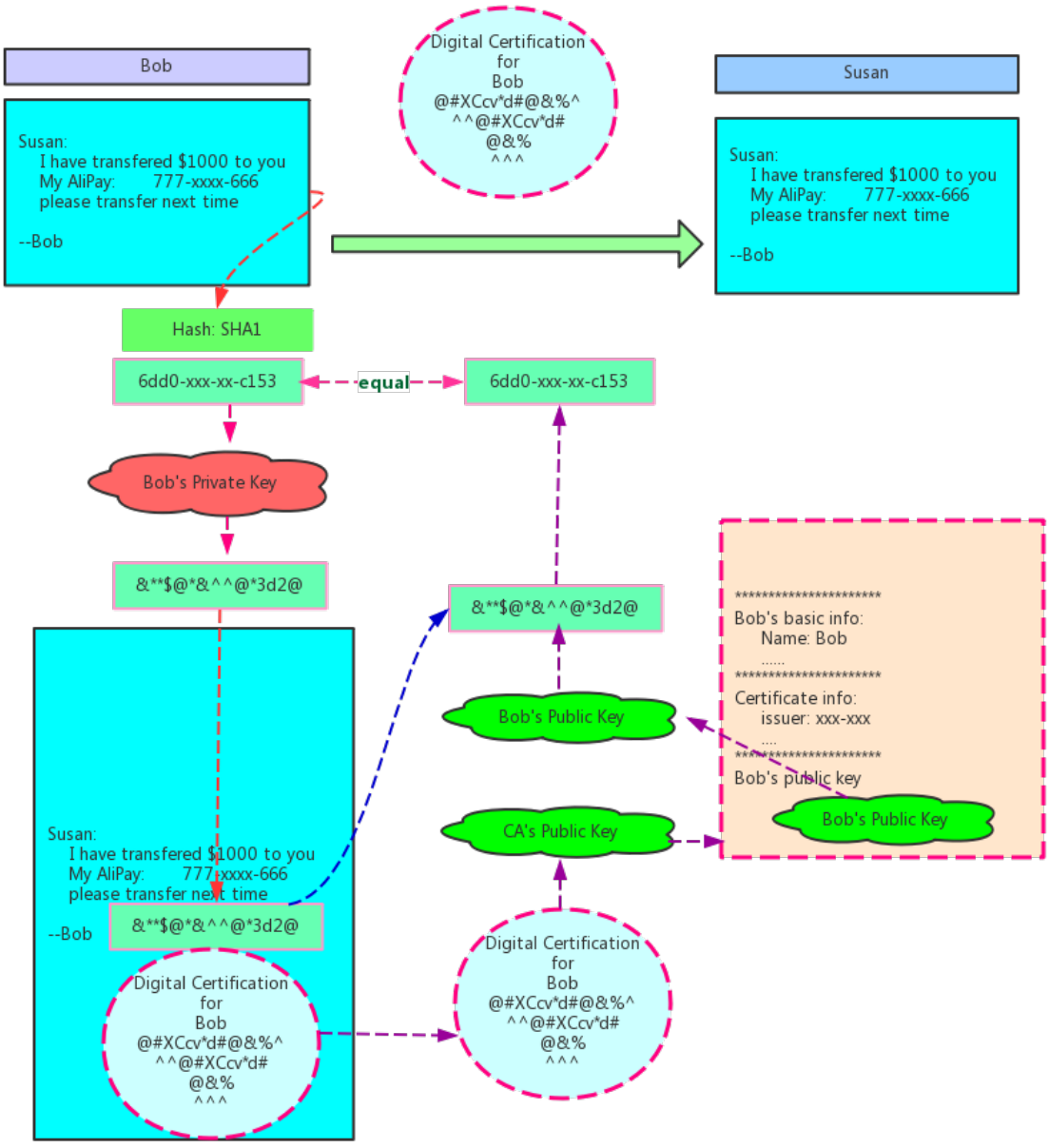
1.4 CA--certificate authority center and Digital certification

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



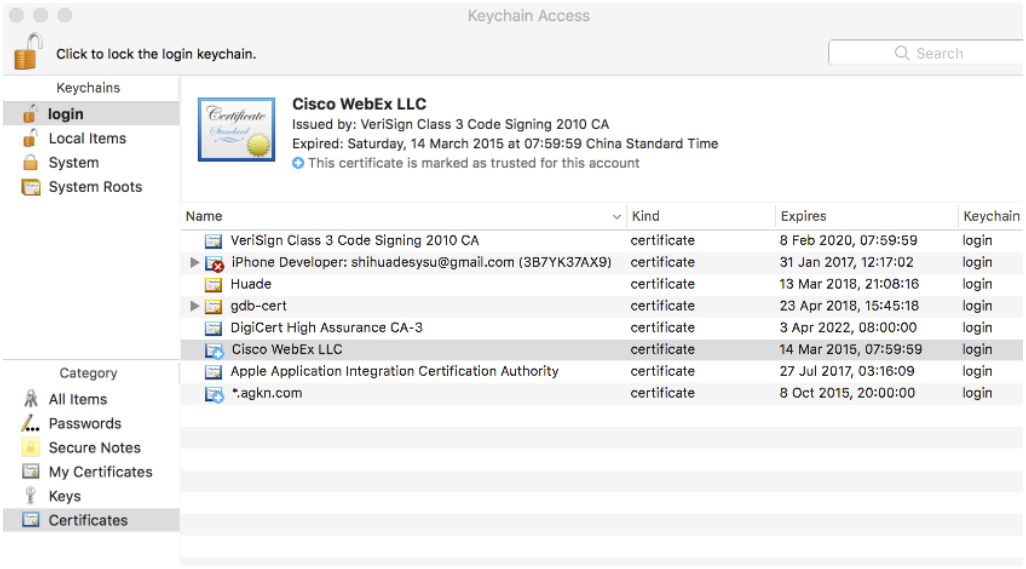
1.5 Communicate based on CA

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

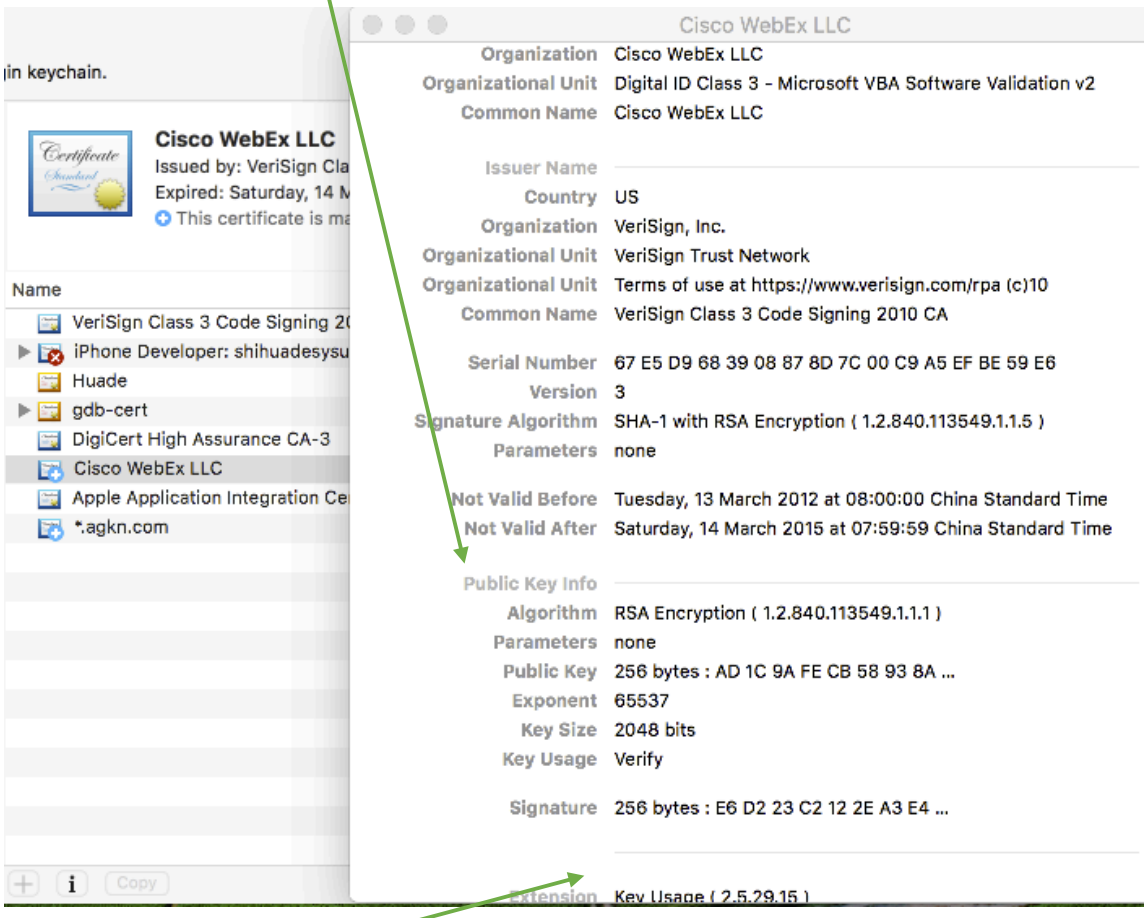


1.6 Example for certification on Mac

Go to keychain access



Public key info for Cisco WebEx LLC

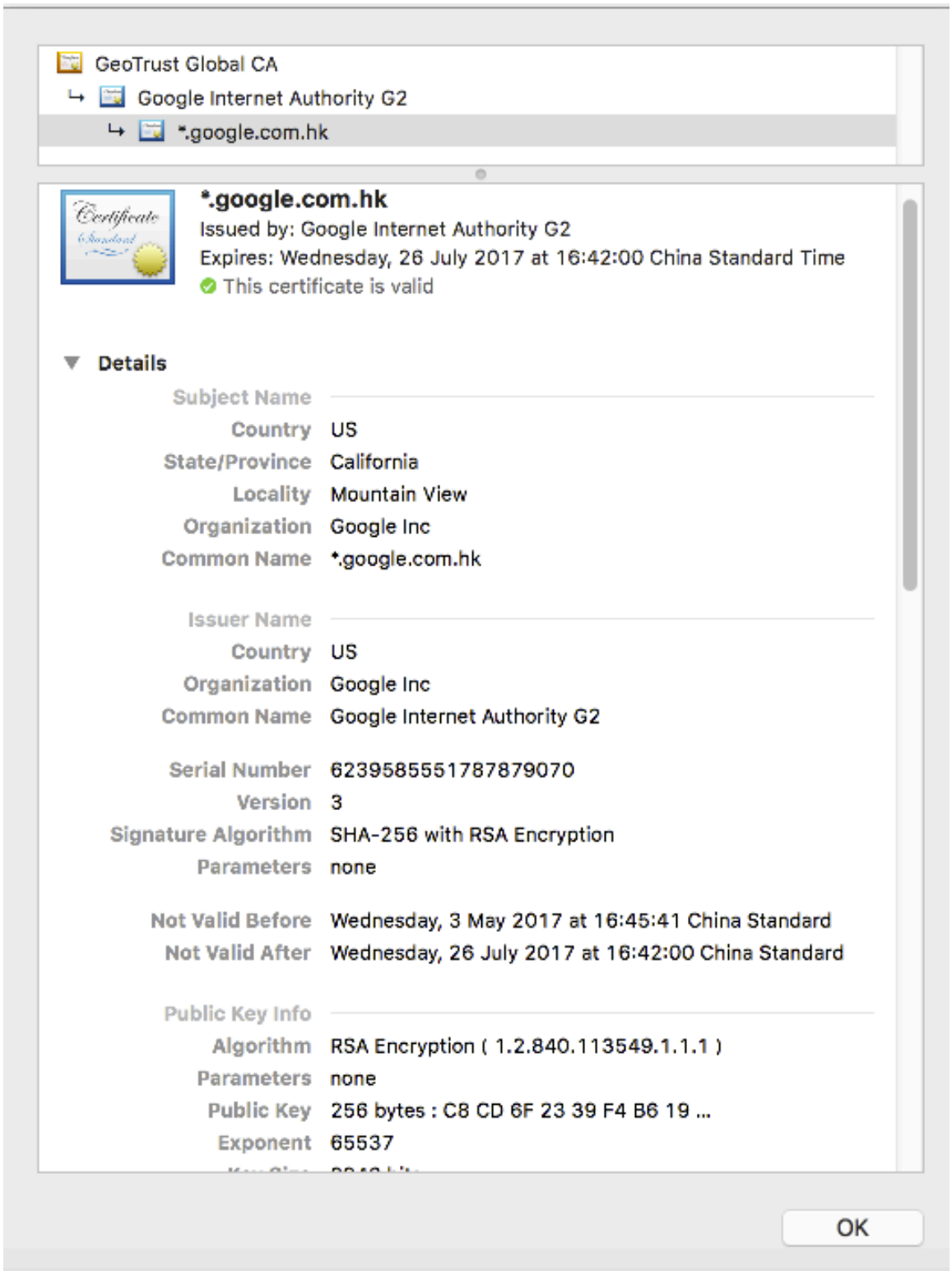


Symantec's CA for Cisco WebExLLC

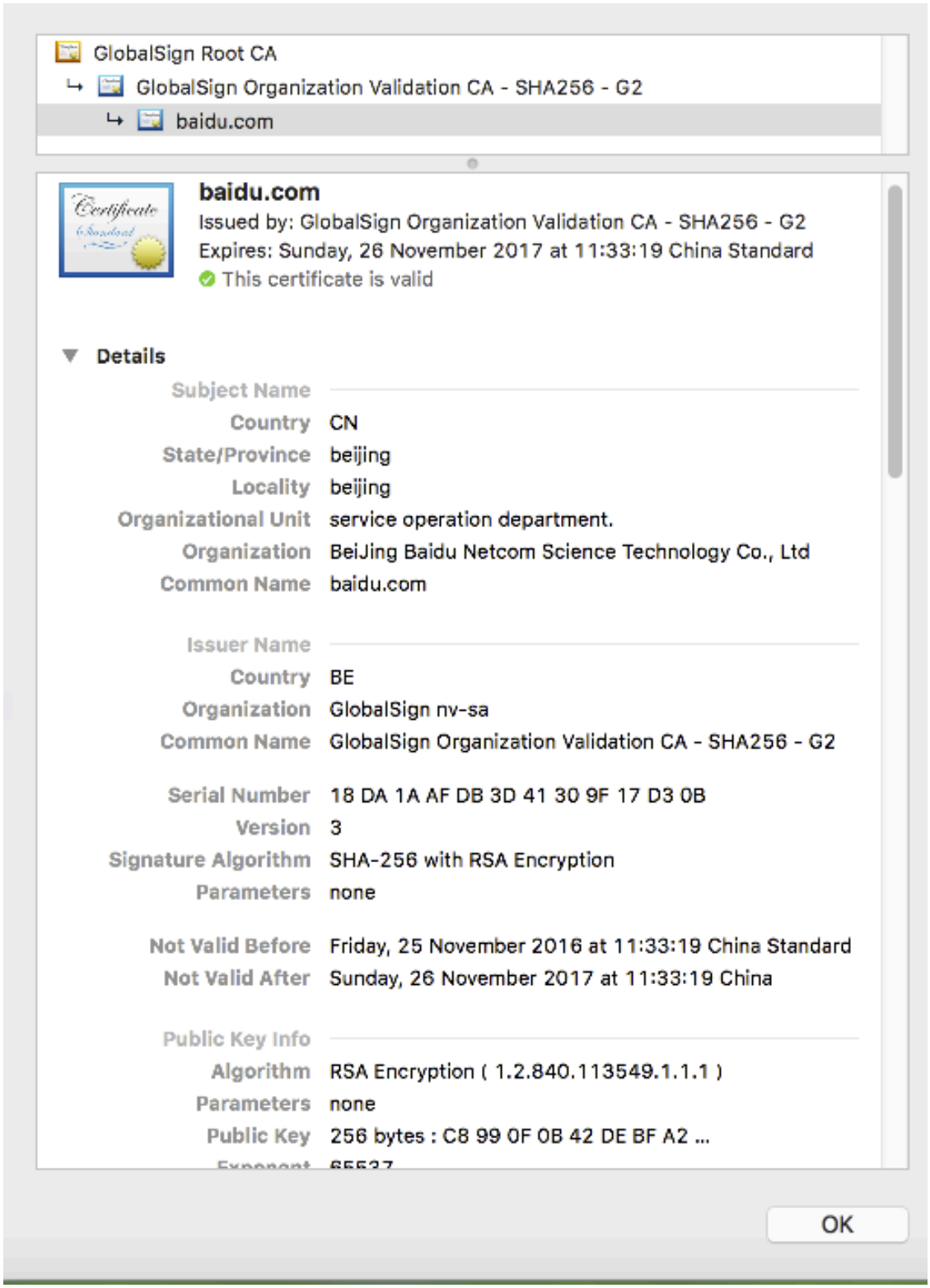
https://www.symantec.com/about/legal/repository.jsp#rpa-ts

1.7 Example for certification on website

Google website:



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

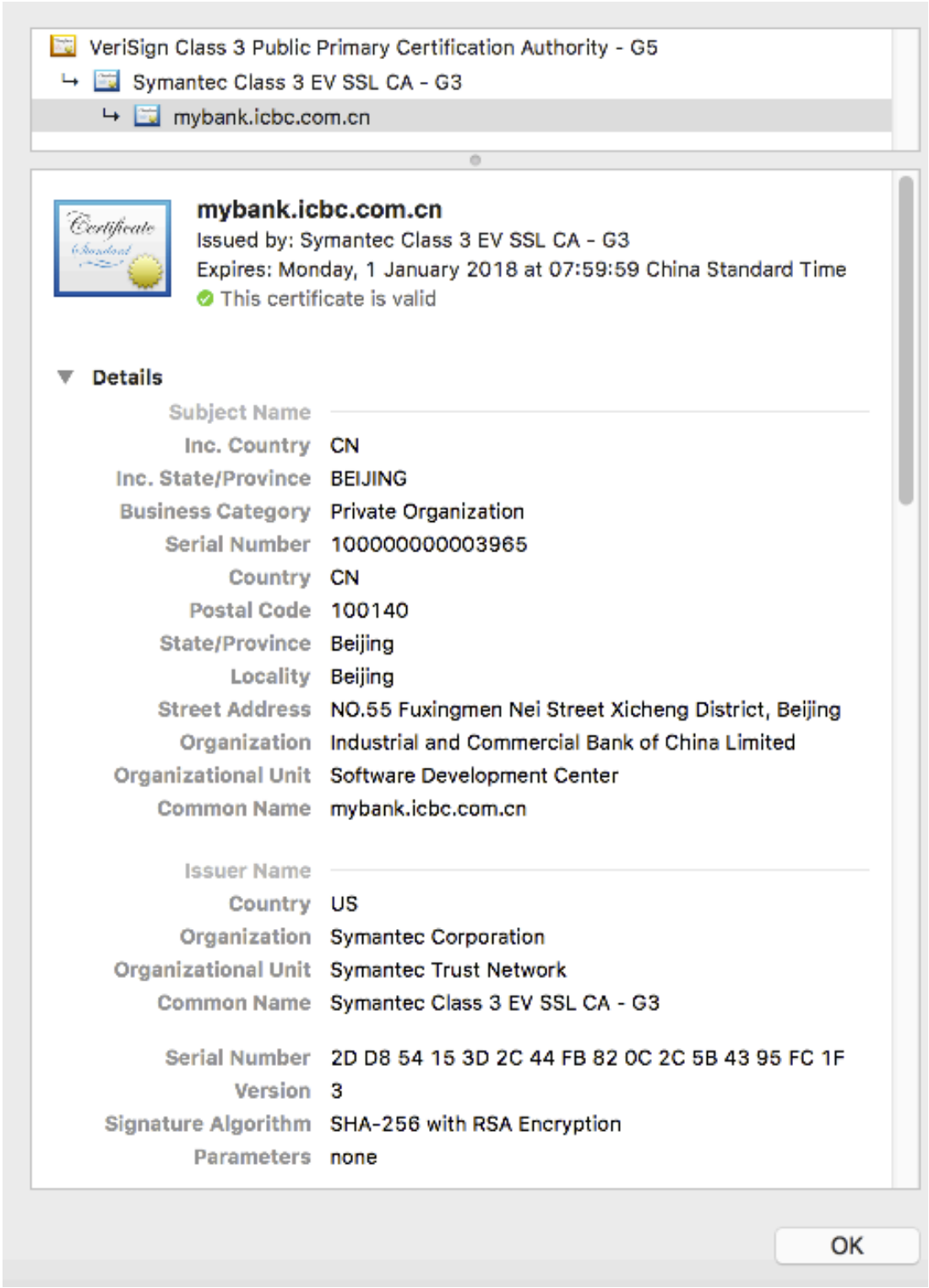


ICBC net bank

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

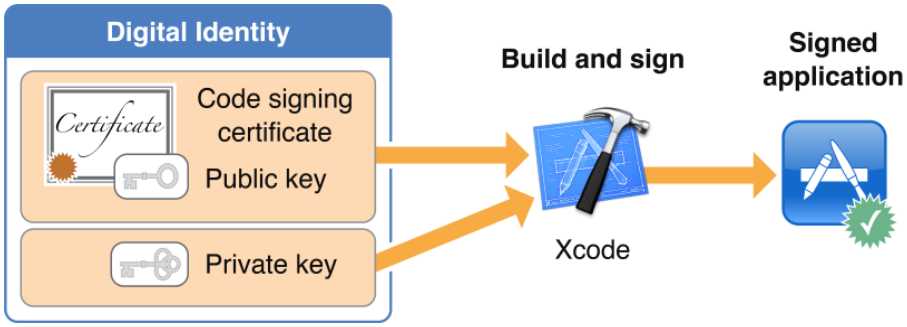


2. Example certification for ios/mac developer

2.1 example

Application Code Signing

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

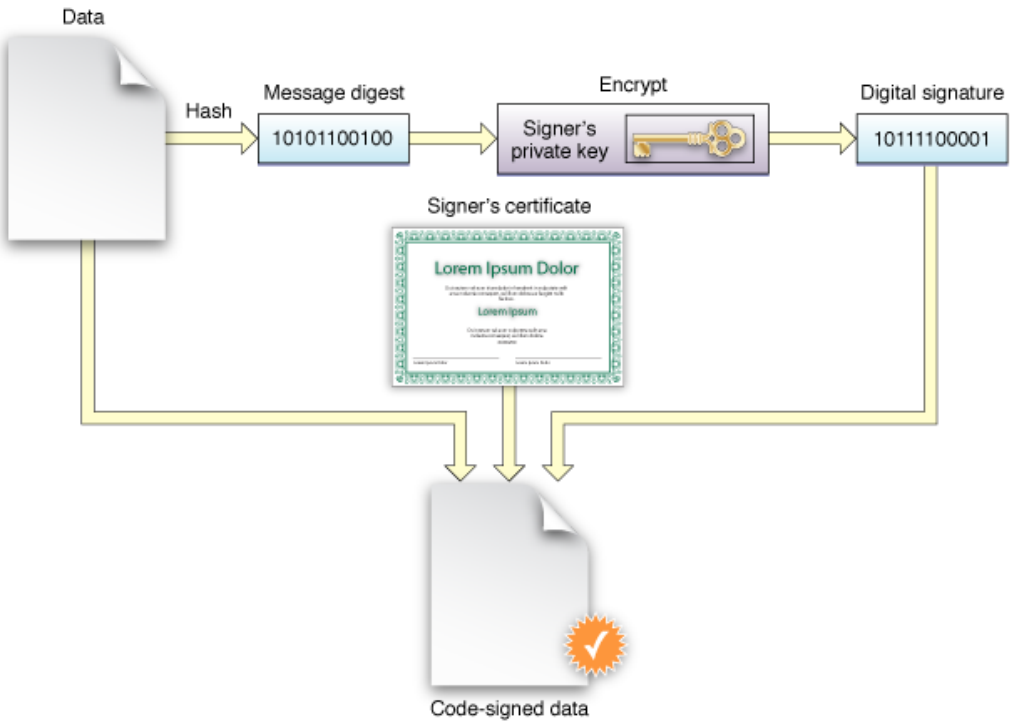


Example in Chinese:

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

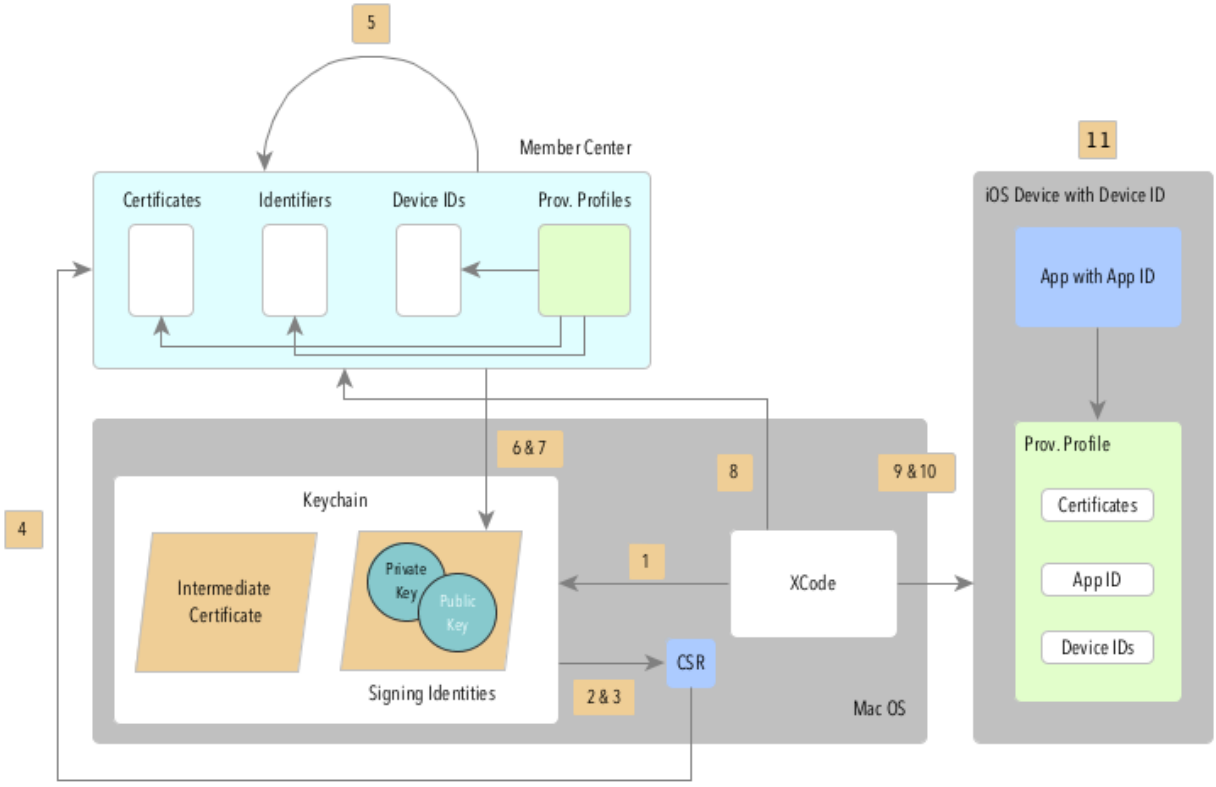
Code signature for mac

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

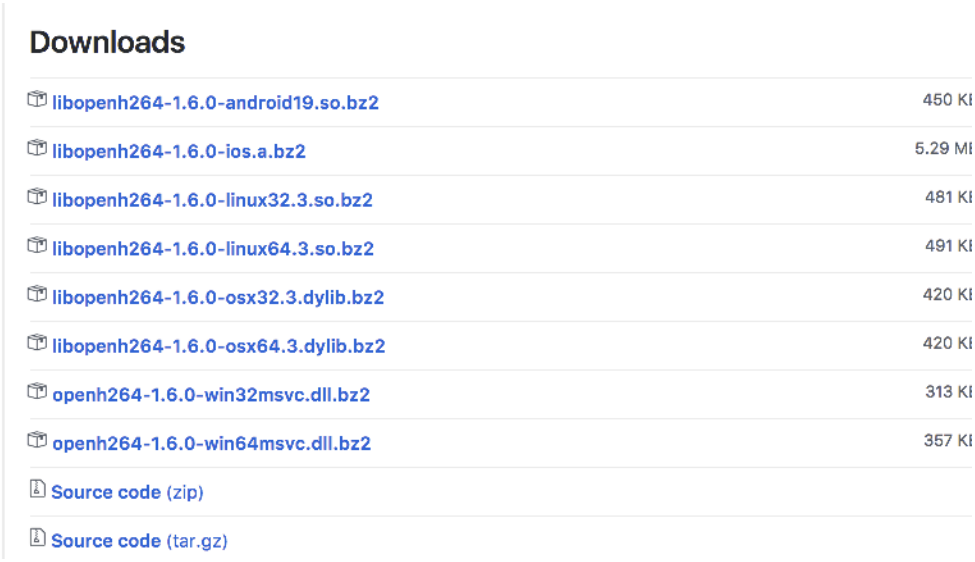
```
HUASHI-M-400W:CodeSignature huashi$ codesign -dv --verbose=4 /Applications/ffmpeg
/Applications/ffmpeg: code object is not signed at all
HUASHI-M-400W:CodeSignature huashi$
```

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



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/