Atitit cer证书的格式与查看，读取生成操作attilax大总结

[1.1. 打开一个cert证书，大部分是txt格式（base64）的，好像也有少部分bin格式。 1](#_Toc20559)

[1.2. 查看证书 运行Windows的证书管理器(到命令行执行certmgr.msc) 1](#_Toc27760)

[1.3. 证书查看器](#_Toc28659) **[SSL安全证书查看（SSLCertStoreViewer）下](#_Toc28659)** [2](#_Toc28659)

[1.4. 需要搞个证书查看器，可以单独选择一个cer证书查看 3](#_Toc20132)

[1.5. 读取cert证书 3](#_Toc25622)

[1.6. 生成cert证书 4](#_Toc1957)

[1.7. 参考资料 4](#_Toc18420)

[1.8. Certificate: 4](#_Toc16893)

[1.9. --------------X509Certificate 12](#_Toc12082)

## 打开一个cert证书，大部分是txt格式（base64）的，好像也有少部分bin格式。

里面就是多个或者一个-----BEGIN CERTIFICATE-----字段。里面包括公钥。。。

-----BEGIN CERTIFICATE-----

MIIC4jCCAkugAwIBAgIQARMLUmh6i/8EkyGUFYilATANBgkqhkiG9w0BAQUFADCB

nzE3MDUGA1UECh4uAEEAbABpAGIAYQBiAGEALgBjAG8AbQAgAEMAbwByAHAAbwBy

AGEAdABpA

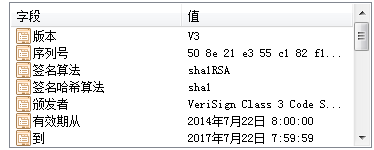
-----END CERTIFICATE-----

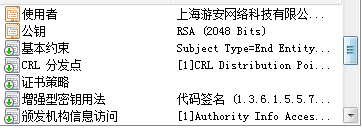
## 查看证书 运行Windows的证书管理器(到命令行执行certmgr.msc)

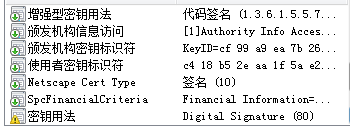
先导入证书，然后在典籍证书的时候，就可以查看他的内容了。

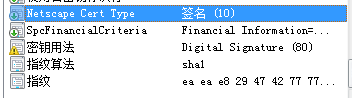
证书overview











但是win 的东东麻烦。

## 证书查看器 **SSL安全证书查看（****SSLCertStoreViewer）下**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Index** | **Cert Store Name** | **Cert Subject Name** | **Cert Issuer Name** | **Issue Date** | **Expiry Date** |
| **1** | **CA Certificates** | **Symantec Class 3 Secure Server CA - G4** | **VeriSign Class 3 Public Primary Certification Authority - G5** | **10/31/2013** | **10/30/2023** |
| **2** | **CA Certificates** | **CFCA Operation CA2** | **CFCA Root CA** | **12/06/2004** | **11/20/2019** |
| **3** | **CA Certificates** | **RapidSSL SHA256 CA** | **GeoTrust Global CA** | **12/11/2013** | **05/20/2022** |
| **4** | **CA Certificates** | **WoSign Class 3 OV Server CA** | **Certification Authority of WoSign** | **08/08/2012** | **08/08/2027** |
| **5** | **CA Certificates** | **VeriSign Class 3 International Server CA - G3** | **VeriSign Class 3 Public Primary Certification Authority - G5** | **02/08/2010** | **02/07/2020** |
| **6** | **CA Certificates** | **GlobalSign Organization Validation CA - SHA256 - G2** | **GlobalSign Root CA** | **02/20/2014** | **02/20/2024** |
| **7** | **CA Certificates** | **GeoTrust SSL CA** | **GeoTrust Global CA** | **02/19/2010** | **02/18/2020** |

**SSLCertStoreViewer也不是很好用，只能选择所有证书，不能选择一个证书查看。。**

## 需要搞个证书查看器，可以单独选择一个cer证书查看

## 读取cert证书

**public** **class** certUtil {

**public** **static** **void** main(String args[]) **throws** Exception {

// 获取X509Certificate的对象

// 从命令行中读入需要验证的证书文件

CertificateFactory of = CertificateFactory.*getInstance*("x.509");

FileInputStream in = **new** FileInputStream("C:\\youan.cer");

java.security.cert.Certificate ceof = of.generateCertificate(in);

System.***out***.println(ceof.getPublicKey().getEncoded() + "\t"

+ ceof.getEncoded());

in.close();

X509Certificate t = (X509Certificate) ceof;

System.***out***.println("Certificate:"+AtiJson.*toJson*(ceof));

System.***out***.println("X509Certificate"+AtiJson.*toJson*(t));

// 获取日期

// 验证证书在某个日期是否有效，从命令行读入年月日，由此生成Date()对象。有Date类的很多设置年月日的方法已经不提倡使用，因此改用Calendar类，Calendar类也是一个工厂类，通过getInstance()方法获得对象，然后使用set()方法设置时间，最后通过其getTime()方法获得Date()对象由于Calendar类的set()方法参数是整数，因此对命令行参数读入的年月日字符串使用Integer.parseInt()方法转换为整数。由于Calendar类的set()方法设置月份时从0开始，0代表1月，11代表12月，因此命令读入的月份要减去1

Calendar cld = Calendar.*getInstance*();

**int** year = Integer.*parseInt*("2012");

**int** month = Integer.*parseInt*("9");

**int** day = Integer.*parseInt*("24");

cld.set(year, month, day);

Date d = cld.getTime();

System.***out***.println(d);

**try** {

// 检验证书

t.checkValidity(d);

## 生成cert证书

|  |  |  |
| --- | --- | --- |
| [java cer证书](https://www.baidu.com/s?wd=java cer%E8%AF%81%E4%B9%A6&rsp=0&f=1&oq=java %E7%94%9F%E6%88%90cer%E8%AF%81%E4%B9%A6&ie=utf-8&f=1&rsv_pq=c5b31ddd0005bf1a&rsv_t=a7f8v0L2GOOi/o+MZOOOzOOqxOgr3K2UD3dMuaygCWO24JsIJJVuPj8TWTY&rqlang=cn&rsv_ers=xn1&rs_src=0&rsv_pq=c5b31ddd0005bf1a&rsv_t=a7f8v0L2GOOi/o+MZOOOzOOqxOgr3K2UD3dMuaygCWO24JsIJJVuPj8TWTY) |  | [keytool 生成cer证书](https://www.baidu.com/s?wd=keytool %E7%94%9F%E6%88%90cer%E8%AF%81%E4%B9%A6&rsp=1&f=1&oq=java %E7%94%9F%E6%88%90cer%E8%AF%81%E4%B9%A6&ie=utf-8&f=1&rsv_pq=c5b31ddd0005bf1a&rsv_t=a7f8v0L2GOOi/o+MZOOOzOOqxOgr3K2UD3dMuaygCWO24JsIJJVuPj8TWTY&rqlang=cn&rsv_ers=xn1&rs_src=0&rsv_pq=c5b31ddd0005bf1a&rsv_t=a7f8v0L2GOOi/o+MZOOOzOOqxOgr3K2UD3dMuaygCWO24JsIJJVuPj8TWTY) |

## 参考资料

公钥证书cer,pfx - 脚踏实地才是最有用的 - 博客频道 - CSDN.NET.html

java 检查本地cer证书(转) - 记录技术点点之路 - ITeye技术网站.html

## Certificate:

{

"authKeyId":{

"identifier":"z5mp6nsm9EvJjo/X8AUm7+PSp50="

},

"authorityInfoAccessExtension":{

"accessDescriptions":[

{

"accessLocation":{

"name":{

"host":"sf.symcd.com",

"hostObject":{

"name":"sf.symcd.com",

"type":2

},

"name":"http://sf.symcd.com",

"scheme":"http",

"type":6,

"uRI":"http://sf.symcd.com"

},

"type":6

},

"accessMethod":{}

},

{

"accessLocation":{

"name":{

"host":"sf.symcb.com",

"hostObject":{

"name":"sf.symcb.com",

"type":2

},

"name":"http://sf.symcb.com/sf.crt",

"scheme":"http",

"type":6,

"uRI":"http://sf.symcb.com/sf.crt"

},

"type":6

},

"accessMethod":{}

}

],

"critical":false,

"elements":["descriptions"],

"extensionId":{},

"extensionValue":"MEkwHwYIKwYBBQUHMAGGE2h0dHA6Ly9zZi5zeW1jZC5jb20wJgYIKwYBBQUHMAKGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3J0",

"id":"1.3.6.1.5.5.7.1.1",

"name":"AuthorityInfoAccess",

"value":"MEkwHwYIKwYBBQUHMAGGE2h0dHA6Ly9zZi5zeW1jZC5jb20wJgYIKwYBBQUHMAKGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3J0"

},

"authorityKeyIdentifierExtension":{

"critical":false,

"elements":["key\_id","auth\_name","serial\_number"],

"extensionId":{},

"extensionValue":"MBaAFM+Zqep7JvRLyY6P1/AFJu/j0qed",

"id":"2.5.29.35",

"name":"AuthorityKeyIdentifier",

"value":"MBaAFM+Zqep7JvRLyY6P1/AFJu/j0qed"

},

"basicConstraints":-1,

"basicConstraintsExtension":{

"critical":false,

"elements":["is\_ca","path\_len"],

"extensionId":{},

"extensionValue":"MAA=",

"id":"2.5.29.19",

"name":"BasicConstraints",

"value":"MAA="

},

"cRLDistributionPointsExtension":{

"critical":false,

"elements":["points"],

"extensionId":{},

"extensionValue":"MCIwIKAeoByGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3Js",

"id":"2.5.29.31",

"name":"CRLDistributionPoints",

"value":"MCIwIKAeoByGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3Js"

},

"certificatePoliciesExtension":{

"critical":false,

"elements":["policies"],

"extensionId":{},

"extensionValue":"MF0wWwYLYIZIAYb4RQEHFwMwTDAjBggrBgEFBQcCARYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9jcHMwJQYIKwYBBQUHAgIwGRYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9ycGE=",

"id":"2.5.29.32",

"name":"CertificatePolicies",

"value":"MF0wWwYLYIZIAYb4RQEHFwMwTDAjBggrBgEFBQcCARYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9jcHMwJQYIKwYBBQUHAgIwGRYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9ycGE="

},

"criticalExtensionOIDs":["2.5.29.15"],

"elements":["x509.info","x509.algorithm","x509.signature","x509.signed\_cert"],

"encoded":"",

"encodedInternal":"",

"extendedKeyUsage":[

"1.3.6.1.5.5.7.3.3"

],

"extendedKeyUsageExtension":{

"critical":false,

"elements":["usages"],

"extendedKeyUsage":[

"1.3.6.1.5.5.7.3.3"

],

"extensionId":{},

"extensionValue":"MAoGCCsGAQUFBwMD",

"id":"2.5.29.37",

"name":"ExtendedKeyUsage",

"value":"MAoGCCsGAQUFBwMD"

},

"issuerDN":{

"commonName":"VeriSign Class 3 Code Signing 2010 CA",

"country":"US",

"empty":false,

"encoded":"MIG0MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xHzAdBgNVBAsTFlZlcmlTaWduIFRydXN0IE5ldHdvcmsxOzA5BgNVBAsTMlRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhIChjKTEwMS4wLAYDVQQDEyVWZXJpU2lnbiBDbGFzcyAzIENvZGUgU2lnbmluZyAyMDEwIENB",

"encodedInternal":"MIG0MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xHzAdBgNVBAsTFlZlcmlTaWduIFRydXN0IE5ldHdvcmsxOzA5BgNVBAsTMlRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhIChjKTEwMS4wLAYDVQQDEyVWZXJpU2lnbiBDbGFzcyAzIENvZGUgU2lnbmluZyAyMDEwIENB",

"name":"CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=\"VeriSign, Inc.\", C=US",

"organization":"VeriSign, Inc.",

"organizationalUnit":"VeriSign Trust Network",

"rFC1779Name":"CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=\"VeriSign, Inc.\", C=US",

"rFC2253CanonicalName":"cn=verisign class 3 code signing 2010 ca,ou=terms of use at https://www.verisign.com/rpa (c)10,ou=verisign trust network,o=verisign\\, inc.,c=us",

"rFC2253Name":"CN=VeriSign Class 3 Code Signing 2010 CA,OU=Terms of use at https://www.verisign.com/rpa (c)10,OU=VeriSign Trust Network,O=VeriSign\\, Inc.,C=US",

"type":4

},

"keyUsage":[true,false,false,false,false,false,false,false,false],

"name":"x509",

"nonCriticalExtensionOIDs":["1.3.6.1.4.1.311.2.1.27","1.3.6.1.5.5.7.1.1","2.16.840.1.113730.1.1","2.5.29.14","2.5.29.19","2.5.29.31","2.5.29.32","2.5.29.35","2.5.29.37"],

"notAfter":1500681599000,

"notBefore":1405987200000,

"publicKey":{

"algorithm":"RSA",

"algorithmId":{

"name":"RSA",

"oID":{}

},

"encoded":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvwvhjYVQlihHlpLmrfx9liOltIcWfqVP+wFer/CEzzXY2L9i27bd74WfrL7BM2BxWI092flXiEJ+ZJ2yROefvGyshCansG78/JXeYTdMwrCVL/uCDAleF3E7ZjPoN5JFHcO9hW0LsP/pqLg+s9aoKdlrPayjYiwdkGOFpz4hAsv8/XSCfJX38za74ECtrmZZN+UUmsDfEVVqtZkp1jtZtxtyPHUiyg9+bQpfva+P1QSAR/JjWcpb3w7z6U7CXeJkCwZfGVVRy/RaLj6IdwpE+2BiMYuFCPjAAG85M0jqRONpyK/Cw9WeQeT5F3LMAUeDDNc/LSUWMjrXPynjn57CHQIDAQAB",

"encodedInternal":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvwvhjYVQlihHlpLmrfx9liOltIcWfqVP+wFer/CEzzXY2L9i27bd74WfrL7BM2BxWI092flXiEJ+ZJ2yROefvGyshCansG78/JXeYTdMwrCVL/uCDAleF3E7ZjPoN5JFHcO9hW0LsP/pqLg+s9aoKdlrPayjYiwdkGOFpz4hAsv8/XSCfJX38za74ECtrmZZN+UUmsDfEVVqtZkp1jtZtxtyPHUiyg9+bQpfva+P1QSAR/JjWcpb3w7z6U7CXeJkCwZfGVVRy/RaLj6IdwpE+2BiMYuFCPjAAG85M0jqRONpyK/Cw9WeQeT5F3LMAUeDDNc/LSUWMjrXPynjn57CHQIDAQAB",

"format":"X.509",

"modulus":24117375020366103769649778688714161391650583047104219683274875765146960329475158788089824533814267922162292507923392239861679152846520206007991995625637077739607407396851494294162990262799636527759347043124896125793405882662045991184066126966654983747162710414560825714673945114630804094784851978354473827717993152108183583504664444059342222934099326876467062156129126229129806662589252938220759934835169448480214121023952848072733537598672104928606718707644232828371441425439416333100048457701877541579993269508449083029447102757568375039079402976615203399779355898361327173175037589197151282703491496254874211762717,

"publicExponent":65537

},

"serialNumber":107076233147555193481415261582109626452,

"serialNumberObject":{

"number":107076233147555193481415261582109626452

},

"sigAlgName":"SHA1withRSA",

"sigAlgOID":"1.2.840.113549.1.1.5",

"signature":"4AmHODNe+jh9LTr+7UJpkDWwddbrTOu2LWGzBK13gbZz/6HbLRgDtEzLPvyuccGnwlyd5F4VOkG1SnLC7QAYAatMPAQQvE4N2I6QX6CbNpG0ChrX4Y6jXCLmZ1kkgojCwkWJgekuS7DeUVpfRCP2z0LBzEayVYaptjDUu+8bN8Ozf42skAiyYXjzWYpGlNc4YPDQ1YGXso/twlvYynIjwNN4ODBtU3mMn7n9UZkOaW84HCP6fThuyW33PA9HOKeYkC845SH9wah9Oi+xqfMmpHZTCAh3aUE/jOxTiEyd17PoDyzTdeMcntgFe/vK0JtdHJOU7Ds7cJxmdvKaabqSPA==",

"subjectDN":{

"commonName":"上海游安网络科技有限公司",

"country":"CN",

"empty":false,

"encoded":"MIGQMQswCQYDVQQGEwJDTjESMBAGA1UECAwJ5LiK5rW35biCMQ8wDQYDVQQHDAbkuIrmtbcxLTArBgNVBAoMJOS4iua1t+a4uOWuiee9kee7nOenkeaKgOaciemZkOWFrOWPuDEtMCsGA1UEAwwk5LiK5rW35ri45a6J572R57uc56eR5oqA5pyJ6ZmQ5YWs5Y+4",

"encodedInternal":"MIGQMQswCQYDVQQGEwJDTjESMBAGA1UECAwJ5LiK5rW35biCMQ8wDQYDVQQHDAbkuIrmtbcxLTArBgNVBAoMJOS4iua1t+a4uOWuiee9kee7nOenkeaKgOaciemZkOWFrOWPuDEtMCsGA1UEAwwk5LiK5rW35ri45a6J572R57uc56eR5oqA5pyJ6ZmQ5YWs5Y+4",

"locality":"上海",

"name":"CN=上海游安网络科技有限公司, O=上海游安网络科技有限公司, L=上海, ST=上海市, C=CN",

"organization":"上海游安网络科技有限公司",

"rFC1779Name":"CN=上海游安网络科技有限公司, O=上海游安网络科技有限公司, L=上海, ST=上海市, C=CN",

"rFC2253CanonicalName":"cn=上海游安网络科技有限公司,o=上海游安网络科技有限公司,l=上海,st=上海市,c=cn",

"rFC2253Name":"CN=上海游安网络科技有限公司,O=上海游安网络科技有限公司,L=上海,ST=上海市,C=CN",

"state":"上海市",

"type":4

},

"subjectKeyId":{

"identifier":"xBi1LqofWuJc+bvewQ6dltTgR6o="

},

"subjectKeyIdentifierExtension":{

"critical":false,

"elements":["key\_id"],

"extensionId":{},

"extensionValue":"BBTEGLUuqh9a4lz5u97BDp2W1OBHqg==",

"id":"2.5.29.14",

"name":"SubjectKeyIdentifier",

"value":"BBTEGLUuqh9a4lz5u97BDp2W1OBHqg=="

},

"tBSCertificate":"",

"type":"X.509",

"version":3

}

## --------------X509Certificate

{

"authKeyId":{

"identifier":"z5mp6nsm9EvJjo/X8AUm7+PSp50="

},

"authorityInfoAccessExtension":{

"accessDescriptions":[

{

"accessLocation":{

"name":{

"host":"sf.symcd.com",

"hostObject":{

"name":"sf.symcd.com",

"type":2

},

"name":"http://sf.symcd.com",

"scheme":"http",

"type":6,

"uRI":"http://sf.symcd.com"

},

"type":6

},

"accessMethod":{}

},

{

"accessLocation":{

"name":{

"host":"sf.symcb.com",

"hostObject":{

"name":"sf.symcb.com",

"type":2

},

"name":"http://sf.symcb.com/sf.crt",

"scheme":"http",

"type":6,

"uRI":"http://sf.symcb.com/sf.crt"

},

"type":6

},

"accessMethod":{}

}

],

"critical":false,

"elements":["descriptions"],

"extensionId":{},

"extensionValue":"MEkwHwYIKwYBBQUHMAGGE2h0dHA6Ly9zZi5zeW1jZC5jb20wJgYIKwYBBQUHMAKGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3J0",

"id":"1.3.6.1.5.5.7.1.1",

"name":"AuthorityInfoAccess",

"value":"MEkwHwYIKwYBBQUHMAGGE2h0dHA6Ly9zZi5zeW1jZC5jb20wJgYIKwYBBQUHMAKGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3J0"

},

"authorityKeyIdentifierExtension":{

"critical":false,

"elements":["key\_id","auth\_name","serial\_number"],

"extensionId":{},

"extensionValue":"MBaAFM+Zqep7JvRLyY6P1/AFJu/j0qed",

"id":"2.5.29.35",

"name":"AuthorityKeyIdentifier",

"value":"MBaAFM+Zqep7JvRLyY6P1/AFJu/j0qed"

},

"basicConstraints":-1,

"basicConstraintsExtension":{

"critical":false,

"elements":["is\_ca","path\_len"],

"extensionId":{},

"extensionValue":"MAA=",

"id":"2.5.29.19",

"name":"BasicConstraints",

"value":"MAA="

},

"cRLDistributionPointsExtension":{

"critical":false,

"elements":["points"],

"extensionId":{},

"extensionValue":"MCIwIKAeoByGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3Js",

"id":"2.5.29.31",

"name":"CRLDistributionPoints",

"value":"MCIwIKAeoByGGmh0dHA6Ly9zZi5zeW1jYi5jb20vc2YuY3Js"

},

"certificatePoliciesExtension":{

"critical":false,

"elements":["policies"],

"extensionId":{},

"extensionValue":"MF0wWwYLYIZIAYb4RQEHFwMwTDAjBggrBgEFBQcCARYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9jcHMwJQYIKwYBBQUHAgIwGRYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9ycGE=",

"id":"2.5.29.32",

"name":"CertificatePolicies",

"value":"MF0wWwYLYIZIAYb4RQEHFwMwTDAjBggrBgEFBQcCARYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9jcHMwJQYIKwYBBQUHAgIwGRYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9ycGE="

},

"criticalExtensionOIDs":["2.5.29.15"],

"elements":["x509.info","x509.algorithm","x509.signature","x509.signed\_cert"],

"encoded":"",

"encodedInternal":"",

"extendedKeyUsage":[

"1.3.6.1.5.5.7.3.3"

],

"extendedKeyUsageExtension":{

"critical":false,

"elements":["usages"],

"extendedKeyUsage":[

"1.3.6.1.5.5.7.3.3"

],

"extensionId":{},

"extensionValue":"MAoGCCsGAQUFBwMD",

"id":"2.5.29.37",

"name":"ExtendedKeyUsage",

"value":"MAoGCCsGAQUFBwMD"

},

"issuerDN":{

"commonName":"VeriSign Class 3 Code Signing 2010 CA",

"country":"US",

"empty":false,

"encoded":"MIG0MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xHzAdBgNVBAsTFlZlcmlTaWduIFRydXN0IE5ldHdvcmsxOzA5BgNVBAsTMlRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhIChjKTEwMS4wLAYDVQQDEyVWZXJpU2lnbiBDbGFzcyAzIENvZGUgU2lnbmluZyAyMDEwIENB",

"encodedInternal":"MIG0MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xHzAdBgNVBAsTFlZlcmlTaWduIFRydXN0IE5ldHdvcmsxOzA5BgNVBAsTMlRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhIChjKTEwMS4wLAYDVQQDEyVWZXJpU2lnbiBDbGFzcyAzIENvZGUgU2lnbmluZyAyMDEwIENB",

"name":"CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=\"VeriSign, Inc.\", C=US",

"organization":"VeriSign, Inc.",

"organizationalUnit":"VeriSign Trust Network",

"rFC1779Name":"CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O=\"VeriSign, Inc.\", C=US",

"rFC2253CanonicalName":"cn=verisign class 3 code signing 2010 ca,ou=terms of use at https://www.verisign.com/rpa (c)10,ou=verisign trust network,o=verisign\\, inc.,c=us",

"rFC2253Name":"CN=VeriSign Class 3 Code Signing 2010 CA,OU=Terms of use at https://www.verisign.com/rpa (c)10,OU=VeriSign Trust Network,O=VeriSign\\, Inc.,C=US",

"type":4

},

"keyUsage":[true,false,false,false,false,false,false,false,false],

"name":"x509",

"nonCriticalExtensionOIDs":["1.3.6.1.4.1.311.2.1.27","1.3.6.1.5.5.7.1.1","2.16.840.1.113730.1.1","2.5.29.14","2.5.29.19","2.5.29.31","2.5.29.32","2.5.29.35","2.5.29.37"],

"notAfter":1500681599000,

"notBefore":1405987200000,

"publicKey":{

"algorithm":"RSA",

"algorithmId":{

"name":"RSA",

"oID":{}

},

"encoded":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvwvhjYVQlihHlpLmrfx9liOltIcWfqVP+wFer/CEzzXY2L9i27bd74WfrL7BM2BxWI092flXiEJ+ZJ2yROefvGyshCansG78/JXeYTdMwrCVL/uCDAleF3E7ZjPoN5JFHcO9hW0LsP/pqLg+s9aoKdlrPayjYiwdkGOFpz4hAsv8/XSCfJX38za74ECtrmZZN+UUmsDfEVVqtZkp1jtZtxtyPHUiyg9+bQpfva+P1QSAR/JjWcpb3w7z6U7CXeJkCwZfGVVRy/RaLj6IdwpE+2BiMYuFCPjAAG85M0jqRONpyK/Cw9WeQeT5F3LMAUeDDNc/LSUWMjrXPynjn57CHQIDAQAB",

"encodedInternal":"MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvwvhjYVQlihHlpLmrfx9liOltIcWfqVP+wFer/CEzzXY2L9i27bd74WfrL7BM2BxWI092flXiEJ+ZJ2yROefvGyshCansG78/JXeYTdMwrCVL/uCDAleF3E7ZjPoN5JFHcO9hW0LsP/pqLg+s9aoKdlrPayjYiwdkGOFpz4hAsv8/XSCfJX38za74ECtrmZZN+UUmsDfEVVqtZkp1jtZtxtyPHUiyg9+bQpfva+P1QSAR/JjWcpb3w7z6U7CXeJkCwZfGVVRy/RaLj6IdwpE+2BiMYuFCPjAAG85M0jqRONpyK/Cw9WeQeT5F3LMAUeDDNc/LSUWMjrXPynjn57CHQIDAQAB",

"format":"X.509",

"modulus":24117375020366103769649778688714161391650583047104219683274875765146960329475158788089824533814267922162292507923392239861679152846520206007991995625637077739607407396851494294162990262799636527759347043124896125793405882662045991184066126966654983747162710414560825714673945114630804094784851978354473827717993152108183583504664444059342222934099326876467062156129126229129806662589252938220759934835169448480214121023952848072733537598672104928606718707644232828371441425439416333100048457701877541579993269508449083029447102757568375039079402976615203399779355898361327173175037589197151282703491496254874211762717,

"publicExponent":65537

},

"serialNumber":107076233147555193481415261582109626452,

"serialNumberObject":{

"number":107076233147555193481415261582109626452

},

"sigAlgName":"SHA1withRSA",

"sigAlgOID":"1.2.840.113549.1.1.5",

"signature":"4AmHODNe+jh9LTr+7UJpkDWwddbrTOu2LWGzBK13gbZz/6HbLRgDtEzLPvyuccGnwlyd5F4VOkG1SnLC7QAYAatMPAQQvE4N2I6QX6CbNpG0ChrX4Y6jXCLmZ1kkgojCwkWJgekuS7DeUVpfRCP2z0LBzEayVYaptjDUu+8bN8Ozf42skAiyYXjzWYpGlNc4YPDQ1YGXso/twlvYynIjwNN4ODBtU3mMn7n9UZkOaW84HCP6fThuyW33PA9HOKeYkC845SH9wah9Oi+xqfMmpHZTCAh3aUE/jOxTiEyd17PoDyzTdeMcntgFe/vK0JtdHJOU7Ds7cJxmdvKaabqSPA==",

"subjectDN":{

"commonName":"上海游安网络科技有限公司",

"country":"CN",

"empty":false,

"encoded":"MIGQMQswCQYDVQQGEwJDTjESMBAGA1UECAwJ5LiK5rW35biCMQ8wDQYDVQQHDAbkuIrmtbcxLTArBgNVBAoMJOS4iua1t+a4uOWuiee9kee7nOenkeaKgOaciemZkOWFrOWPuDEtMCsGA1UEAwwk5LiK5rW35ri45a6J572R57uc56eR5oqA5pyJ6ZmQ5YWs5Y+4",

"encodedInternal":"MIGQMQswCQYDVQQGEwJDTjESMBAGA1UECAwJ5LiK5rW35biCMQ8wDQYDVQQHDAbkuIrmtbcxLTArBgNVBAoMJOS4iua1t+a4uOWuiee9kee7nOenkeaKgOaciemZkOWFrOWPuDEtMCsGA1UEAwwk5LiK5rW35ri45a6J572R57uc56eR5oqA5pyJ6ZmQ5YWs5Y+4",

"locality":"上海",

"name":"CN=上海游安网络科技有限公司, O=上海游安网络科技有限公司, L=上海, ST=上海市, C=CN",

"organization":"上海游安网络科技有限公司",

"rFC1779Name":"CN=上海游安网络科技有限公司, O=上海游安网络科技有限公司, L=上海, ST=上海市, C=CN",

"rFC2253CanonicalName":"cn=上海游安网络科技有限公司,o=上海游安网络科技有限公司,l=上海,st=上海市,c=cn",

"rFC2253Name":"CN=上海游安网络科技有限公司,O=上海游安网络科技有限公司,L=上海,ST=上海市,C=CN",

"state":"上海市",

"type":4

},

"subjectKeyId":{

"identifier":"xBi1LqofWuJc+bvewQ6dltTgR6o="

},

"subjectKeyIdentifierExtension":{

"critical":false,

"elements":["key\_id"],

"extensionId":{},

"extensionValue":"BBTEGLUuqh9a4lz5u97BDp2W1OBHqg==",

"id":"2.5.29.14",

"name":"SubjectKeyIdentifier",

"value":"BBTEGLUuqh9a4lz5u97BDp2W1OBHqg=="

},

"tBSCertificate":"",

"type":"X.509",

"version":3

}

Wed Oct 24 12:24:53 CST 2012

Too early

NotBefore: Tue Jul 22 08:00:00 CST 2014