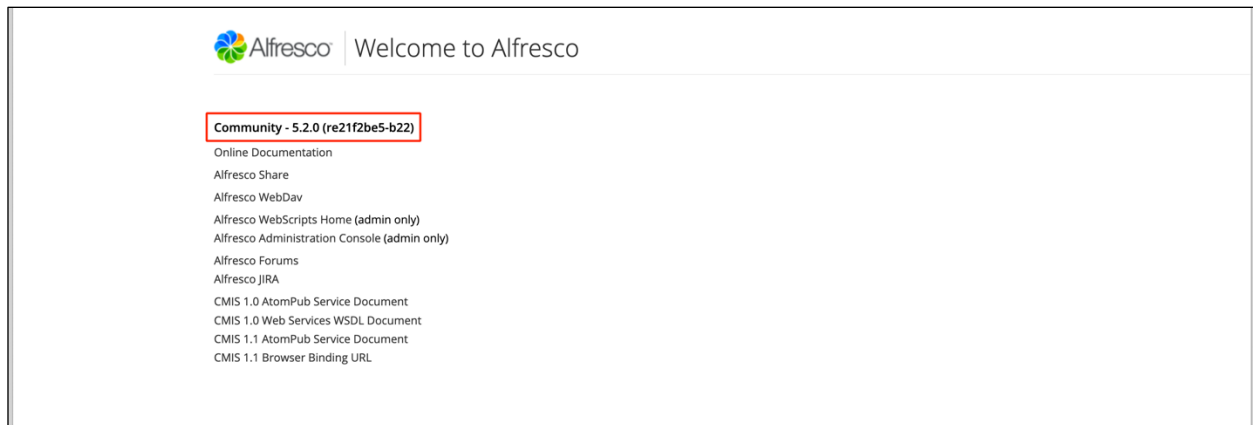


Alfresco Disclosures

Software Version 5.2 - General Release: 201707

Environment:

- Alfresco Community - Version 5.2 - General Release: 201707
- Windows and Ubuntu
- Easy Install options used (default)



Findings:

1. CVE-2019-14222: Default Certificate

Description:

Alfresco Community 5.x and below ships by default with a set of known private certificates. Anyone who downloads and installs the Alfresco Community software on a local machine gets access to these files.

Once obtained, these private keys can be used to:

- Gain access to Solr (which uses x509 certificate authentication)
- Launch active MITM attacks using a trusted Alfresco Certificate
- Launch passive decryption attacks if Non-Ephemeral ciphers are used

Requirements:

For gaining access to Solr:

- Access to an TLS/SSL port hosting solr (443, 8443, etc.)
- The server still uses the default private cert

For decrypting client - server traffic:

- Active MITM attack
- Passive MITM attack with non-Ephemeral cipher

Proof of Concept:

1.1. Gain access to the Solr application used by Alfresco:

By importing the “browser.p12” file into the browser (password: alfresco), an attacker can use it to authenticate to any Solr Server that still uses this default certificate.

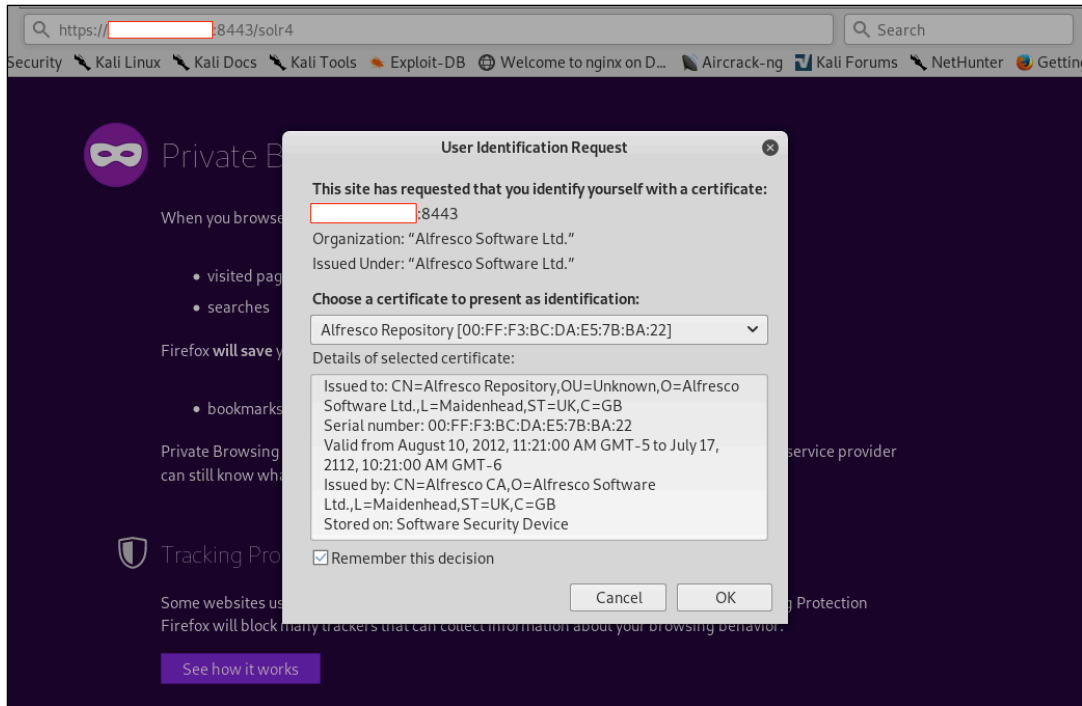


Figure 1. Browser Asks for Certificate Authentication

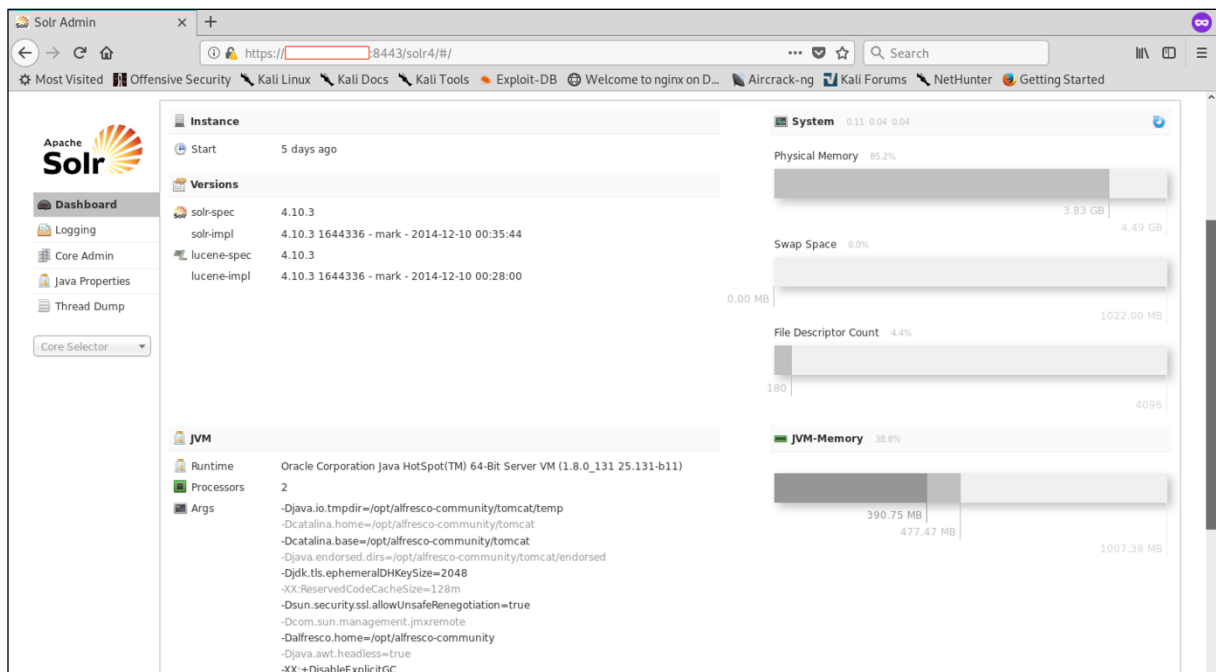


Figure 2. Successful Authentication to Solr Admin

1.2. Perform Active Man-In-The-Middle attacks using trusted cert, or in some edge cases, decrypt captured traffic (if non-ephemeral ciphers were used):

The following images will be presenting the second case (decryption of captured traffic) in Wireshark:

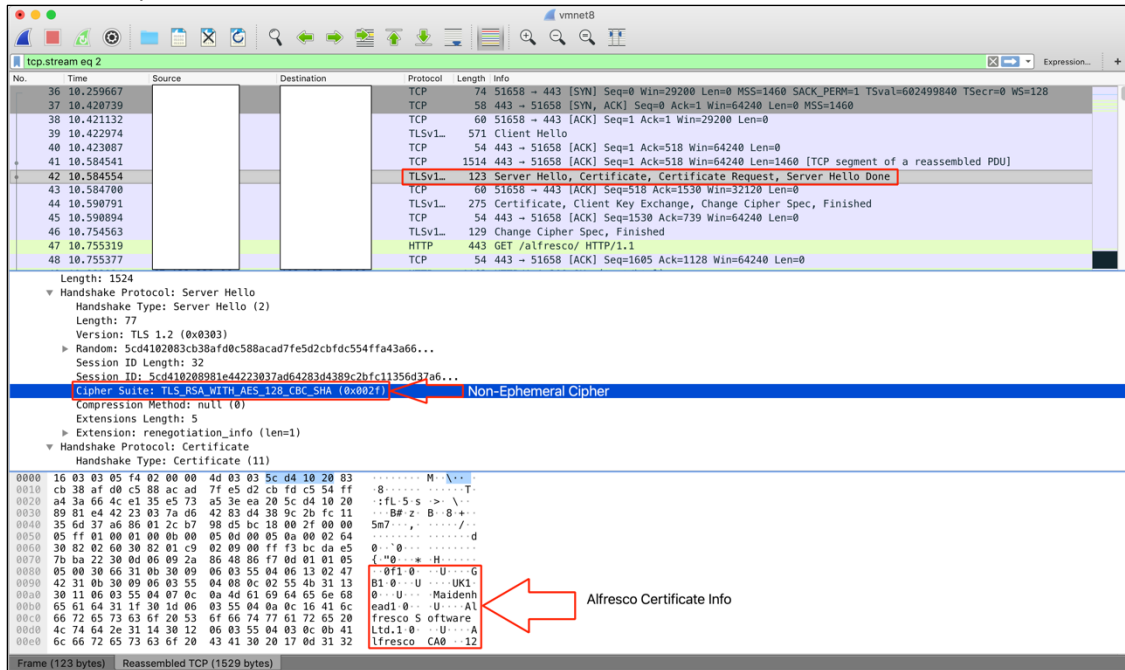


Figure 3. Establishing TLS with Unsafe Cipher and Alfresco Certificate

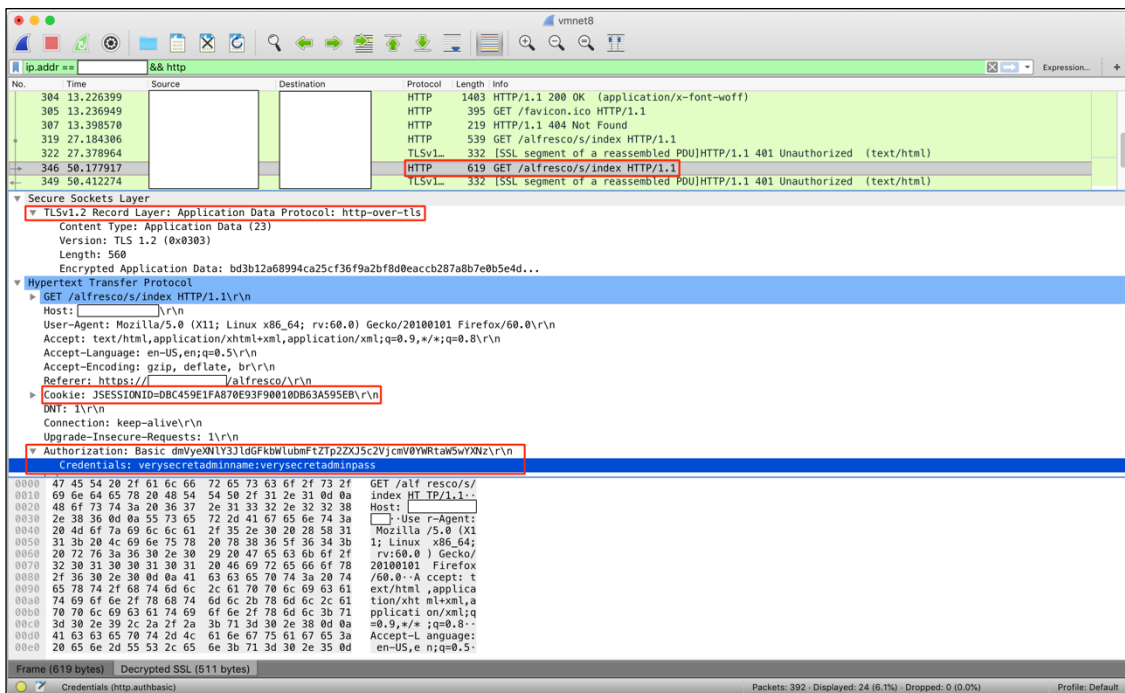
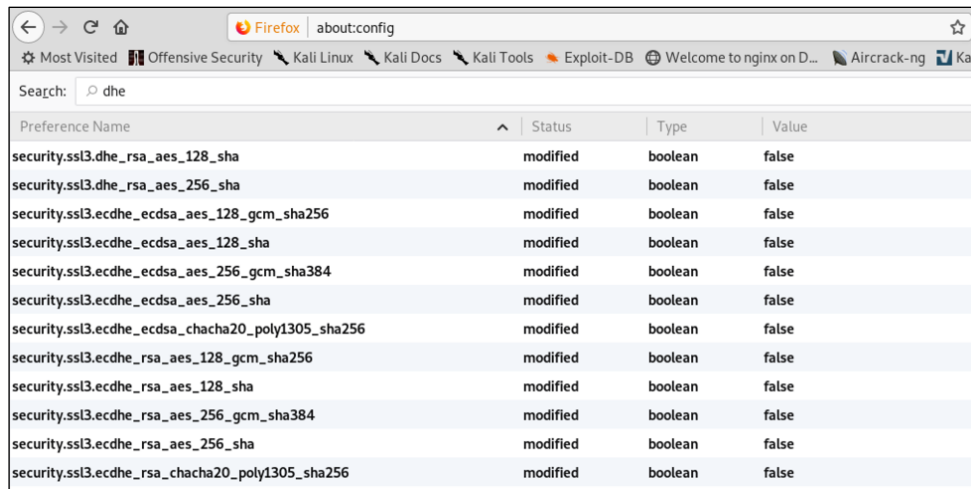


Figure 4. Decrypted Traffic using Private Key

Note: This was made possible because the target server supported Non-Ephemeral Ciphers, as well as the fact that the browser used for testing purposes was configured to use these unsafe ciphers.



The screenshot shows the Firefox 'about:config' page with a search filter of 'dhe'. A list of 13 security settings is displayed, all of which have been manually modified to 'false'. These settings pertain to various TLS cipher suites, specifically those involving Diffie-Hellman (DHE) or Elliptic Curve Diffie-Hellman (ECDHE) key exchange. The browser's status bar at the top shows several open tabs, including 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Welcome to nginx on D...', 'Aircrack-ng', and 'Kal'.

Preference Name	Status	Type	Value
security.ssl3.dhe_rsa_aes_128_sha	modified	boolean	false
security.ssl3.dhe_rsa_aes_256_sha	modified	boolean	false
security.ssl3.ecdsa_aes_128_gcm_sha256	modified	boolean	false
security.ssl3.ecdsa_aes_128_sha	modified	boolean	false
security.ssl3.ecdsa_aes_256_gcm_sha384	modified	boolean	false
security.ssl3.ecdsa_aes_256_sha	modified	boolean	false
security.ssl3.ecdsa_chacha20_poly1305_sha256	modified	boolean	false
security.ssl3.ecdhe_rsa_aes_128_gcm_sha256	modified	boolean	false
security.ssl3.ecdhe_rsa_aes_128_sha	modified	boolean	false
security.ssl3.ecdhe_rsa_aes_256_gcm_sha384	modified	boolean	false
security.ssl3.ecdhe_rsa_aes_256_sha	modified	boolean	false
security.ssl3.ecdhe_rsa_chacha20_poly1305_sha256	modified	boolean	false

Figure 5. Unsafe Browser Settings used for Testing Purposes

Appendix:

Alfresco RSA Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKqBgQCX67H7604bPWaBpmfSrQMlQamw/25gGpH9skaKOIv0gHDXzYRY
KRvGusQwHEdpf2IE5PoSPcsbmc7T6fqHsCcUjtE5qTv56i+qTz6FBFoh5VWZjBJG
HRs6VLQ8Jk9Emz73cgod9fUR+xqquGQ59SYce0yrnCUseytGW3irqYKiwiDAQAB
AoGARvYdCOL8dNTVULH9xPZzha+KJ9boI5PFpY7kTCPlm6tzChpBOzzYcJdElIRd
/bM2gbrC5Epg2N+bMHkWQNMtLVgUISR0pSeqGgCDEdbRVnk8xxRnwdEwQbu+fv95
PNCmZkVb5Wv1qr4afpYspzsZlC/aU0cDoVsyLUhO6q1/YsEQQDqmdVNnCo3HgHj
D5bcygywpTbRiUojGyS10Syt1fw2Snbwj7+T0mgAgPcTnDjx3aUT0LT70Hrww4Th
6bQ84YP5AkEApchYFKjuEgJKPIG8Mk61+S0nrYhL8yiz8aSEiEtJDC7Q4/B+f3rA
bSjVHl0zCw0yhFmhLVuADJy2Qx9EwLHbowJBAN0LZvomgNU8gGLfy0OPZDhJ7odQ
eIbni4+qBAhLdFppj/3uRJbA/jGbYU8nK5aTbo3Vq09G1N5mbInamYHaxWECQDdE
StjYWEV4rfbt6Sd8Rf4Dp66aOXeeoh50kho9vuRo1wqmKgWljnDVo/cHukGM7Mji
fvD84CAAsXjaSPgFFsBECQF7s1WinVNcNiRB2+Lt1XQuZLmadHDR1E7MoVqpUkG7K
TISWmCrQOIakdAwfKJNvt0akKb0BB1450cE6XbqVLUM=
-----END RSA PRIVATE KEY-----
```

OpenSSL info for Browser PKCS12, password “alfresco”:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBAGBqhkKiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwDgQIJeF5tsQo3BUCAgGA
MBQGCCqGSIb3DQMHBBAguLtgcwC9MgSCAoAspi427fDT5Mtwg/xOiSrO468C/H4k
gSWbCEifENCTWHbhSpFlvkGHnYwN+NPgmq4SGBYJ9fx1D7iX7H8T9jFVHrJgDzCu
lT3g8qzHta/vFImmPNCJfIUAQpSTKmqepnXJA/3ecdQFPc7ojZc7urkhK67I8tz8
ua9ijRP1/riPhRCTsiygNA5N83nRL0pmdDkoxG0Fz+I9vJnpOUztOzeL2ki5hJEY
bIRHEtp2J96wACK4ZKFoOylAmD+XvqZQPWnh7NPsemW37bTgrqv9EBcHx3Go0lfo
ii6m84ir6YpGrxyMNowk2rXxwVGPoDa4OWC3CE/RdFM4QacSCAJY6EMcyfeWQ895
296Y8zgPeDuVaP0qifXP8qQA0S2Eh23q+1XWBk3XezJ6+CMY4NwAB4+767RQuB8C
7rJLc3kOor7tpiVtv40S2LQyD+glyVBP29qQ8U5bjN/wutxwPehK2RWULzUzsDho
J0Iot65WizfZY6Ypso4vPbraR9q5XSAZ0yYTgw2cXLOe2yqHoxEW2U8/pVCxbtQs
GSqihYLIRoVeOUyuvYZCK7LVsjxlQVp2Ms5oH/jFZcjgQceh4tFmSv/dqrZAW3Jw
IGdYLL6EUImzjZYBC4PNxXrAJ9mgPe6SUjuQrUqchdwPUFjpdawtJ4/JbSAAbpZX
TSJPCxR30ffSnQk8EE+KmwOelfpd7t78KXzoXEapILJMsOP593OgxtSCxZrCt8lm
ooY5y4EA3s1bPnP1Zx10i71GN1/OWtT8PoIvuNllyVSyUaRqF22RRuF7rd8REhNW
ZpbMoy5wGrm+IAGIEqfQaneeSrBBm5pwIvtYIETjBPTSbt2nnn9ev4gB
-----END ENCRYPTED PRIVATE KEY-----
Bag Attributes
    friendlyName: CN=Alfresco Repository,OU=Unknown,O=Alfresco Software Ltd.,L=Maidenhead,ST=UK,C=GB
    localKeyID: 54 69 6D 65 20 31 33 34 34 37 35 38 38 33 38 35 39 33
subject=/C=GB/ST=UK/L=Maidenhead/O=Alfresco Software Ltd./OU=Unknown/CN=Alfresco Repository
issuer=/C=GB/ST=UK/L=Maidenhead/O=Alfresco Software Ltd./CN=Alfresco CA
-----BEGIN CERTIFICATE-----
MIICYDCCAcCkCCQD/87za5Xu6IjANBgkqhkiG9w0BAQUFADBMMQswCQYDVQQGEwJH
QjEELMAkGA1UECABWCVUuSExZARBgNVBAcMCKlhaWRlbmhlYWQwH2AdBgNVBAoMFkFs
ZnJlc2NvIFNvZnR3YXJlIEU0ZC4xZDAsBgNVBAMMC0FsZnJlc2NvIENBMCAXDTEy
MDgxMDE2MjEwMmF0YDZlIxtIwNzE3MTYyMTAwWjCBGDELMakGA1UEBhMCR0IxCzAJ
BgNVBAGTA1VLMRMEQYDVQQQHEwvYXN5bWlkZW50ZWZkMR8wHQYDVQKEExZBbGZyZXNj
byBtB2Z0d2FyZSBMDGQuMRAWdgYDVQQLLEwdVbmtub3duMRwwGgYDVQQDEXNBbGZy
ZXNjb3BzZXVvc210b3J5MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX67H7
604bPWaBpmfSrQMlQamw/25gGpH9skaKOIv0gHDXzYRYKRvGusQwHEdpf2IE5PoS
Pcsbmc7T6fqHsCcUjtE5qTv56i+qTz6FBFoh5VWZjBJGHRs6VLQ8Jk9Emz73cgod
9fUR+xqquGQ59SYce0yrnCUseytGW3irqYKiwiDAQABMA0GCSqGSIb3DQEBBQUA
A4GBAGAN0/9mLAmCF6LgYFumyodYZmzqUGDTvaCyIBC56stSe4Z+WuM0/oaTzwXg
KfksudPBGABfBKkH0rNqB1h4YIUxdsgNhojVSUBK5qzd10xykKH/70uHIE2ZZ3u
FnFuvKYPP1Oh6doy0bkeZhDgJUK587YT19L/URAGuvd4osgz
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: CN=Alfresco CA,O=Alfresco Software Ltd.,L=Maidenhead,ST=UK,C=GB
subject=/C=GB/ST=UK/L=Maidenhead/O=Alfresco Software Ltd./CN=Alfresco CA
issuer=/C=GB/ST=UK/L=Maidenhead/O=Alfresco Software Ltd./CN=Alfresco CA
-----BEGIN CERTIFICATE-----
MIICnDCCAgWgAwIBAgIJAILUY/ZsJjzXMA0GCSqGSIb3DQEBBQUAMGYxCzAJBgNV
BAYTAkdCMQswCQYDVQQIDAJVSzETMBEGA1UEBwwKTWFPZGVuaGVhZDEFMBOGA1UE
CgwWQWxmcmVzY28gU29mdHdhcmUgTHRkLjEUMBIGA1UEAwQLQWxmcmVzY28gQ0Ew
IbCNMTIwODEwMTYxNzM0WhgPMjExMjA3MTcxNjE3MzRaMGYxCzAJBgNVBAYTAkdC
MQswCQYDVQQIDAJVSzETMBEGA1UEBwwKTWFPZGVuaGVhZDEFMBOGA1UECgwWQWxm
cmVzY28gU29mdHdhcmUgTHRkLjEUMBIGA1UEAwQLQWxmcmVzY28gQ0EwZ8WdQYJ
KoZ1hvcNAQEBBQADgY0AMIGJAoGBAOoocnTBBh88zAbsNUb292F4HgwE/4jqyBnU
I/uj2Js6247Sulcm91jgbiKly6ZC+sGeTwBQoJ67/tNS4f/Gibc4SuUnIooFvnP
NbpRnebzWkCuxiK9gApzRtmqAJrgaTOBIBV3P0QB5snD8Uc5ZwhCgf3joXtn73Kj
yZFgJXnXAgMBAAGjUDBOMB0GA1UdDgQWBBDGp8/OEY7gLx9BhR/2wiMheoV2TAF
BgNVSMEDAwgBQDGP8/OEY7gLx9BhR/2wiMheoV2TAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4GBAKKwXcAeLn+viE+iXTIN1SHxRBDJ4+zW2N7C1heJ1om3
ONNNB03H1dZFY0L3kj5UC25KF0/wxEbG6Fb6On+j7AggXxYbLTqrTJP57qLTja
gyoEHBeZHL+ZLVQz4+934/5yO7qNdH/6cu38VctGbQfrqfwxgCJ5L5OpK2U3sVrk
-----END CERTIFICATE-----
```