OpenSSL을 윈도우에서 사용하는 방법을 한국 사이트에서 찾다가 너무 복잡하거나 안되는 방법으로 써놔서 조금 고생했다.

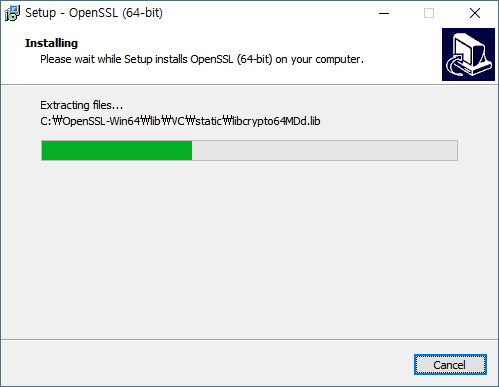
   내가 참고한 사이트는 다음과 같다.

<https://www.tbs-certificates.co.uk/FAQ/en/openssl-windows.html>

<http://rietta.com/blog/2012/01/27/openssl-generating-rsa-key-from-command/>

**1. 설치**

   다운로드 ☞ <http://slproweb.com/products/Win32OpenSSL.html>



   위 사이트로 가서 Win32(or 64) OpenSSL과 Visual C++ 2008 Redistributables를 다운로드 받는다.

   OpenSSL은 32와 64중에 하나만 받으면 되고, 되도록이면 최신 버전으로 다운받을 것을 권한다. Visual C++ 2008 Redistributables는 다운로드 후에 next~ next~버튼을 누르는 인스톨 과정을 거치면 된다. 별로 어렵지 않으니 자세한 화면 캡쳐 같은 것은 생략한다.

   OpenSSL 압축 파일을 풀어서 "C:\OpenSSL-Win64"에 위치시킨다.(다른 곳에 해도 상관은 없다)

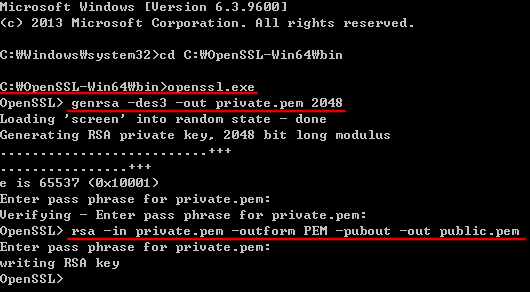
   만약 다운로드 받은 OpenSSL이 1.0 버전이라면, "openssl.cnf" 파일이 필요하다.

[[http://t1.daumcdn.net/tistory_admin/blogs/image/extension/unknown.gif?_version_=9f2eeda506fddd630f86d898c426c44ff9de17db](http://zero-gravity.tistory.com/attachment/cfile9.uf@26467433542231DA12C012.cnf)openssl.cnf](http://zero-gravity.tistory.com/attachment/cfile9.uf@26467433542231DA12C012.cnf)

   해당 파일을 "C:\OpenSSL-Win64" 안에 넣는다.

   자, 이제 준비는 끝났다.

**2. RSA 키 생성**



   RSA 키 생성은 bin 폴더 안에 있는 openssl.exe을 이용한다.

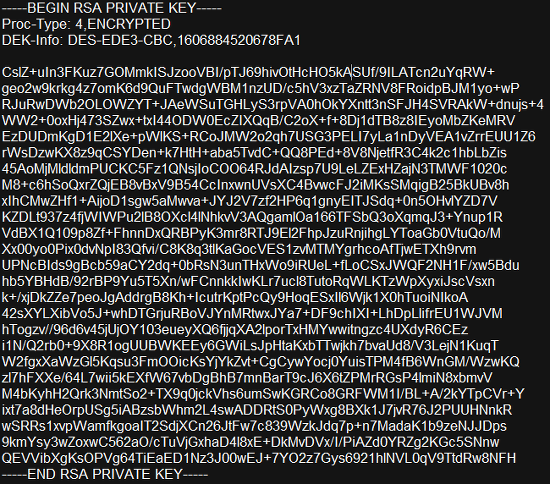
   위에 나처럼 openssl.exe를 호출한 다음에 명령어를 써도 되고, 그냥 바로 명령어 앞에 "openssl"을 붙여서 사용해도 된다.

genrsa -des3 -out private.pem 2048

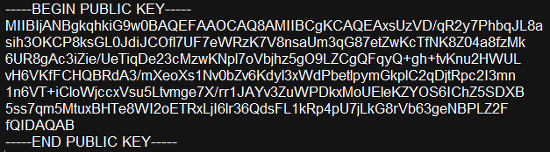
   먼저 private 키를 생성한다. **비밀번호를 입력하고** 나면, bin 폴더 안에 해당 pem 파일이 생긴 것을 확인할 수 있을 것이다. 참고로 2048은 bit 수이다.

   이 키를 갖고 public 키를 생성하는데, 명령어는 다음과 같다.

rsa -in private.pem -outform PEM -pubout -out public.pem



▲ private.pem



▲ public.pem

   에디터로 생성한 private.pem과 public.pem을 열어보면 이렇게 생겼다. 이런 식으로 만들어졌다면 성공!

# openssl 생성관련 정리정보 공유

<http://cf.omnicns.co.kr/pages/viewpage.action?pageId=43876367>

[Skip to end of metadata](http://cf.omnicns.co.kr/pages/viewpage.action?pageId=43876367#page-metadata-end)

* Created by [박병준](http://cf.omnicns.co.kr/display/%7Epppcom7), last modified on [2015-12-29](http://cf.omnicns.co.kr/pages/diffpagesbyversion.action?pageId=43876367&selectedPageVersions=11&selectedPageVersions=12)

[Go to start of metadata](http://cf.omnicns.co.kr/pages/viewpage.action?pageId=43876367#page-metadata-start)

**(openssl 서명 알고리즘 sha2 방식으로 생성하는 요령 아래 URL 참고)**

# 참고사이트  
<http://techglimpse.com/sha256-hash-certificate-openssl/>

# generate x509 SHA256  
openssl req -config openssl.cnf -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout 127.0.0.1.key -out 127.0.0.1.crt

# verify sha256  
openssl x509 -noout -text -in 127.0.0.1.crt

(sample) 생성된 인증서파일

|  |
| --- |
| [127.0.0.1.crt](http://cf.omnicns.co.kr/download/attachments/43876367/127.0.0.1.crt?version=1&modificationDate=1427877216000&api=v2) | | [pppcom7@omnitel.co.kr](mailto:pppcom7@omnitel.co.kr)  비밀번호 : 1234 |
| [127.0.0.1.key](http://cf.omnicns.co.kr/download/attachments/43876367/127.0.0.1.key?version=1&modificationDate=1427877227000&api=v2) | |  |

* 위 생성된 인증서 반영  
  (서명 알고리즘 : **sha256RSA**, 서명 해시 알고리즘 : **sha256**, 공개 키 : **RSA (2048 Bits)**)

(openssl 서명 알고리즘 sha1의 경우 보안 취약점 발생. 앞으로 사설 인증서 생성 시 sha1 알고리즘을 사용하면 안 됨.)

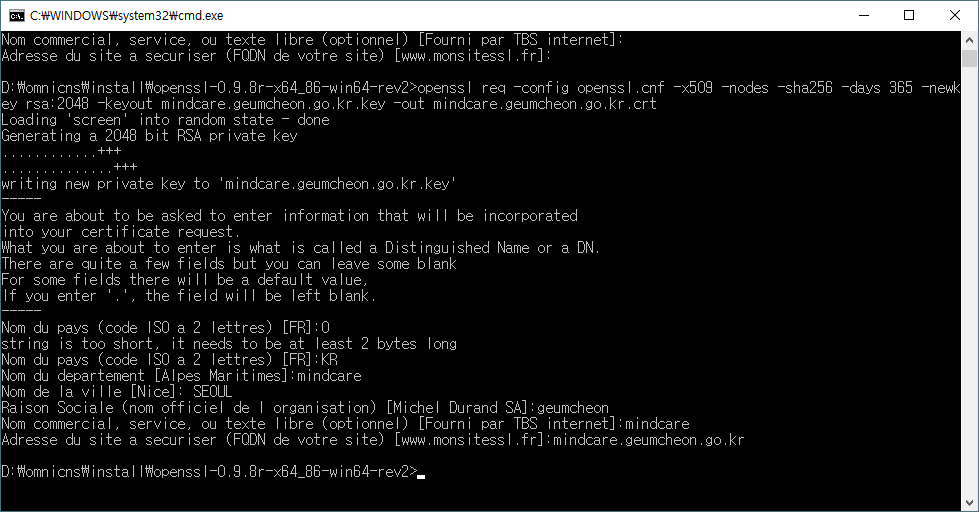
|  |
| --- |
| 개발기 | | https://180.210.196.203:39901 | [180.210.196.203.cert](http://cf.omnicns.co.kr/download/attachments/43876367/180.210.196.203.cert?version=2&modificationDate=1359035711000&api=v2) [180.210.196.203.csr](http://cf.omnicns.co.kr/download/attachments/43876367/180.210.196.203.csr?version=2&modificationDate=1359035711000&api=v2) [180.210.196.203.key](http://cf.omnicns.co.kr/download/attachments/43876367/180.210.196.203.key?version=2&modificationDate=1359035711000&api=v2) |
| 개발기 | | https://211.63.1.210:49901 | [180.210.196.203.cert](http://cf.omnicns.co.kr/download/attachments/43876367/180.210.196.203.cert?version=2&modificationDate=1359035711000&api=v2) [180.210.196.203.csr](http://cf.omnicns.co.kr/download/attachments/43876367/180.210.196.203.csr?version=2&modificationDate=1359035711000&api=v2) [180.210.196.203.key](http://cf.omnicns.co.kr/download/attachments/43876367/180.210.196.203.key?version=2&modificationDate=1359035711000&api=v2) |
| 상용기 | | https://192.168.112.93:39901 | [192.168.112.93.cert](http://cf.omnicns.co.kr/download/attachments/43876367/192.168.112.93.cert?version=1&modificationDate=1359035711000&api=v2) [192.168.112.93.csr](http://cf.omnicns.co.kr/download/attachments/43876367/192.168.112.93.csr?version=1&modificationDate=1359035711000&api=v2) [192.168.112.93.key](http://cf.omnicns.co.kr/download/attachments/43876367/192.168.112.93.key?version=1&modificationDate=1359035711000&api=v2) |
| 상용기  SHA256 | | 2015-12-28 SHA256  서명 알고리즘 적용 | [192.168.112.93\_sha256.zip](http://cf.omnicns.co.kr/download/attachments/43876367/192.168.112.93_sha256.zip?version=1&modificationDate=1451357742000&api=v2) |

openssl 생성 참고 문서 : [참고사이트\_자료.pdf](http://cf.omnicns.co.kr/download/attachments/43876367/%EC%B0%B8%EA%B3%A0%EC%82%AC%EC%9D%B4%ED%8A%B8_%EC%9E%90%EB%A3%8C.pdf?version=1&modificationDate=1359035711000&api=v2)

OpenSSL 공식사이트 : <http://www.openssl.org/source/>  (dll 다운로드)  
64bit용 openssl dll 파일 (v0.9.8.r) : [openssl-0.9.8r-x64\_86-win64-rev2.zip](http://cf.omnicns.co.kr/download/attachments/43876367/openssl-0.9.8r-x64_86-win64-rev2.zip?version=1&modificationDate=1381475731000&api=v2)

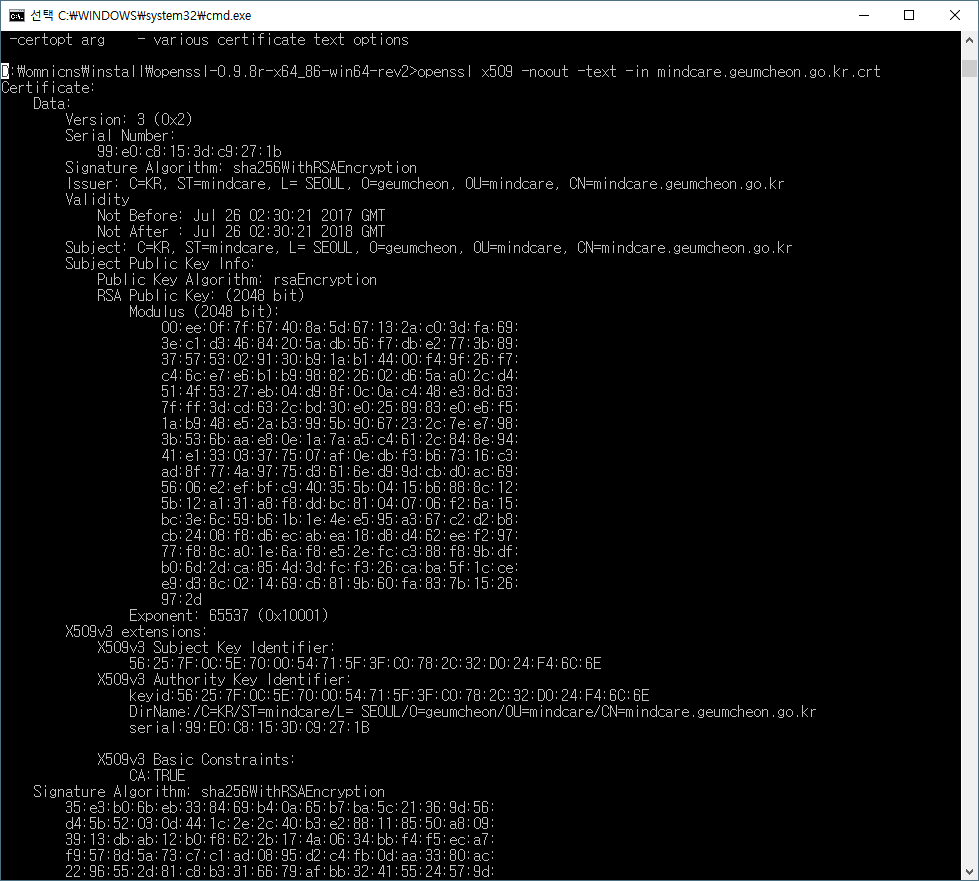
- 인증서 정보 확인

<https://www.kicassl.com/sslcert/sslseccerttool/formSslSecCertToolCsrDecoder.sg>



|  |
| --- |
| Nom du pays (code ISO a 2 lettres) [FR]:KR  Nom du departement [Alpes Maritimes]:mindcare  Nom de la ville [Nice]: SEOUL  Raison Sociale (nom officiel de l organisation) [Michel Durand SA]:geumcheon  Nom commercial, service, ou texte libre (optionnel) [Fourni par TBS internet]:mindcare  Adresse du site a securiser (FQDN de votre site) [www.monsitessl.fr]:mindcare.geumcheon.go.kr |

openssl x509 -noout -text -in mindcare.geumcheon.go.kr.crt



|  |
| --- |
| D:\omnicns\install\openssl-0.9.8r-x64\_86-win64-rev2>openssl x509 -noout -text -in mindcare.geumcheon.go.kr.crt  Certificate:  Data:  Version: 3 (0x2)  Serial Number:  99:e0:c8:15:3d:c9:27:1b  Signature Algorithm: sha256WithRSAEncryption  Issuer: C=KR, ST=mindcare, L= SEOUL, O=geumcheon, OU=mindcare, CN=mindcare.geumcheon.go.kr  Validity  Not Before: Jul 26 02:30:21 2017 GMT  Not After : Jul 26 02:30:21 2018 GMT  Subject: C=KR, ST=mindcare, L= SEOUL, O=geumcheon, OU=mindcare, CN=mindcare.geumcheon.go.kr  Subject Public Key Info:  Public Key Algorithm: rsaEncryption  RSA Public Key: (2048 bit)  Modulus (2048 bit):  00:ee:0f:7f:67:40:8a:5d:67:13:2a:c0:3d:fa:69:  3e:c1:d3:46:84:20:5a:db:56:f7:db:e2:77:3b:89:  37:57:53:02:91:30:b9:1a:b1:44:00:f4:9f:26:f7:  c4:6c:e7:e6:b1:b9:98:82:26:02:d6:5a:a0:2c:d4:  51:4f:53:27:eb:04:d9:8f:0c:0a:c4:48:e3:8d:63:  7f:ff:3d:cd:63:2c:bd:30:e0:25:89:83:e0:e6:f5:  1a:b9:48:e5:2a:b3:99:5b:90:67:23:2c:7e:e7:98:  3b:53:6b:aa:e8:0e:1a:7a:a5:c4:61:2c:84:8e:94:  41:e1:33:03:37:75:07:af:0e:db:f3:b6:73:16:c3:  ad:8f:77:4a:97:75:d3:61:6e:d9:9d:cb:d0:ac:69:  56:06:e2:ef:bf:c9:40:35:5b:04:15:b6:88:8c:12:  5b:12:a1:31:a8:f8:dd:bc:81:04:07:06:f2:6a:15:  bc:3e:6c:59:b6:1b:1e:4e:e5:95:a3:67:c2:d2:b8:  cb:24:08:f8:d6:ec:ab:ea:18:d8:d4:62:ee:f2:97:  77:f8:8c:a0:1e:6a:f8:e5:2e:fc:c3:88:f8:9b:df:  b0:6d:2d:ca:85:4d:3d:fc:f3:26:ca:ba:5f:1c:ce:  e9:d3:8c:02:14:69:c6:81:9b:60:fa:83:7b:15:26:  97:2d  Exponent: 65537 (0x10001)  X509v3 extensions:  X509v3 Subject Key Identifier:  56:25:7F:0C:5E:70:00:54:71:5F:3F:C0:78:2C:32:D0:24:F4:6C:6E  X509v3 Authority Key Identifier:  keyid:56:25:7F:0C:5E:70:00:54:71:5F:3F:C0:78:2C:32:D0:24:F4:6C:6E  DirName:/C=KR/ST=mindcare/L= SEOUL/O=geumcheon/OU=mindcare/CN=mindcare.geumcheon.go.kr  serial:99:E0:C8:15:3D:C9:27:1B  X509v3 Basic Constraints:  CA:TRUE  Signature Algorithm: sha256WithRSAEncryption  35:e3:b0:6b:eb:33:84:69:b4:0a:65:b7:ba:5c:21:36:9d:56:  d4:5b:52:03:0d:44:1c:2e:2c:40:b3:e2:88:11:85:50:a8:09:  39:13:db:ab:12:b0:f8:62:2b:17:4a:06:34:bb:f4:f5:ec:a7:  f9:57:8d:5a:73:c7:c1:ad:08:95:d2:c4:fb:0d:aa:33:80:ac:  22:96:55:2d:81:c8:b3:31:66:79:af:bb:32:41:55:24:57:9d:  5a:74:1c:de:54:58:89:47:c6:d6:ad:15:6f:f9:e9:85:16:71:  92:19:22:6c:3c:43:b3:53:55:6b:b5:4a:af:a0:10:9d:1c:2c:  29:0a:c9:22:ab:0e:b9:7c:37:5b:d6:eb:67:ad:b1:c1:9e:ad:  a3:84:3e:95:c6:70:7c:ad:48:83:4a:c2:33:fb:58:cc:f9:75:  5f:4a:69:1d:69:6b:10:3c:a8:06:e6:ce:50:7e:34:8c:33:77:  3c:88:62:9f:4f:bd:ac:42:45:8c:ea:ea:8c:da:35:18:6e:c4:  8a:0f:d1:cc:3a:d1:31:4d:45:97:34:b0:83:b7:26:93:d6:76:  ab:da:02:62:3e:93:be:64:d8:ba:46:4b:e8:33:9d:e6:cf:f7:  3b:d2:ab:1c:29:a6:78:0e:b9:5c:5b:50:97:8b:7e:28:14:ee:  c2:8b:50:6f |