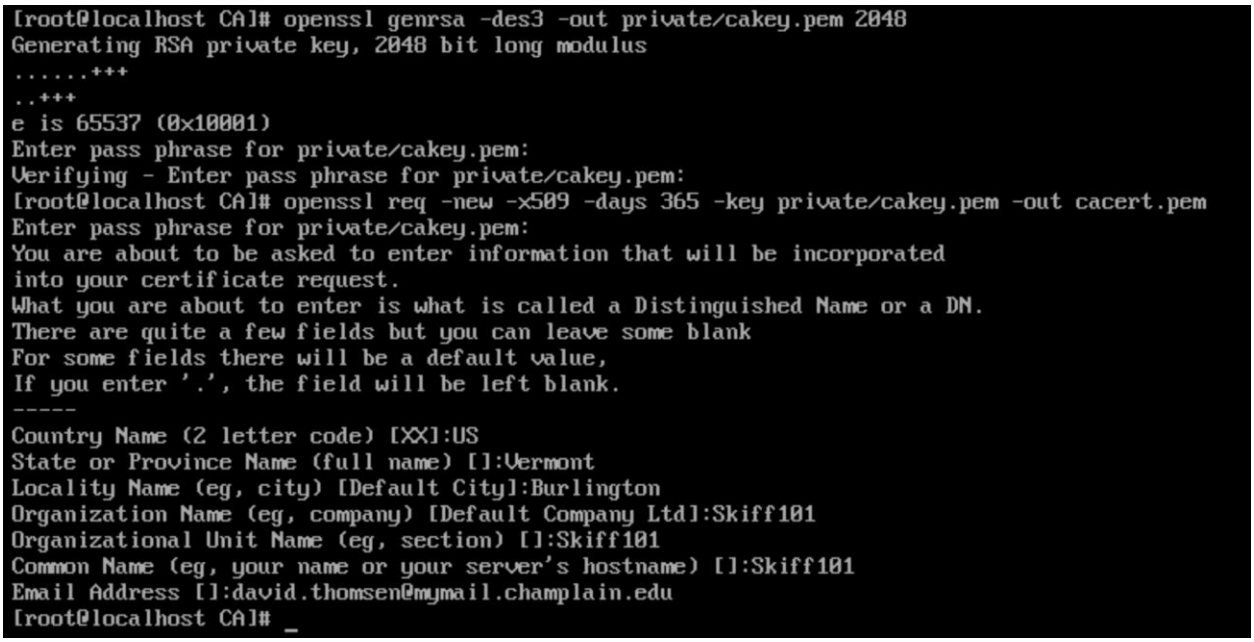
David Thomsen
SEC-260

openssl genrsa -des3 -out private/cakey.pem 2048

This command generates an rsa key then saves it to the private directory.



```
[root@localhost CA]# openssl req -newkey rsa:2048 -keyout websrv.key -out websrv.csr
Generating a 2048 bit RSA private key
.+++
.....................................+++
writing new private key to 'websrv.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Vermont
Locality Name (eg, city) [Default City]:Burlington
Organization Name (eg, company) [Default Company Ltd]:Skiff101
Organizational Unit Name (eg, section) []:Skiff101
Common Name (eg, your name or your server's hostname) []:Skiff101
Email Address []:david.thomsen@mymail.champlain.edu

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@localhost CA]# _
```

```
[root@localhost CA]# cat cacert.pem
-----BEGIN CERTIFICATE-----
MIIEFTCCAv2gAwIBAgIJAIAQfTWFgoN5MA0GCSqGSIb3DQEBCwUAMIGgMQswCQYD
VQQGEwJVUzEQMA4GA1UECAwHVmVybW9udDETMBEGA1UEBwwKQnVybGluZ3RvbjER
MA8GA1UECgwIU2tpZmYxMDExETAPBgNVBAsMCFNraWZmMTAxMREwDwYDVQQDDAhT
a2lmZjEwMTExMC8GCSqGSIb3DQEJARYiZGF2aWQudGhvbXNlbkBteW1haWwuY2hh
bXBsYWluLmVkdTAeFw0yMjAyMTQxMjE4MjZaFw0yMzAyMTQxMjE4MjZaMIGgMQsw
CQYDVQQGEwJVUzEQMA4GA1UECAwHVmVybW9udDETMBEGA1UEBwwKQnVybGluZ3Rv
bjERMA8GA1UECgwIU2tpZmYxMDExETAPBgNVBAsMCFNraWZmMTAxMREwDwYDVQQD
DAhTa2lmZjEwMTExMC8GCSqGSIb3DQEJARYiZGF2aWQudGhvbXNlbkBteW1haWwu
Y2hhbXBsYWluLmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKT6
U+8Gl5idQwpgsP/+C1aoWfv4CRhsYIUEzqDLPUEXoCR1GvVcmzxFrbSfMU0AgwlF
1PhlP84ojKNy0AWd8r1ojx3Vx8CDYQQQfuB/9qGXMRysevepJ46X1BcjOGdufPA7
AKzX5g5s8wiCKti2Xd/YhB5UnfEpSyiordjIvA2dU/S7wdzNL1VuUNxoYb8AFXfg
UTQFbHWNpOBInx3x0n7NMsFqLlKvEJu84c0q318U0PDTmc38d+mJGJ59h41yEawS
IZG+Q+yFREFuPj2WN13AUv6qaDzeWnB2hRclRXB0CLCRy/blUa8qtc0MZKl6VCzI
lEo+vsveB2W7ZZZ83QkCAwEAAaNQME4wHQYDVR0OBBYEFH4o/soHm1t9ZXUKjo1q
RPXd4xl0MB8GA1UdIwQYMBaAFH4o/soHm1t9ZXUKjo1qRPXd4xl0MAwGA1UdEwQF
MAMBAf8wDQYJKoZIhvcNAQELBQADggEBABKQwOPiOnb7Ke9KTSGY1oFZ/Ff2XSOF
vt2hI5ugdABANoYDSXdihp1+7F8yfrifoAl4NXoHVVExs/HaFAO3bNmqemjIw4U0
48BojGavciTHEYgMm5qc4eVjJ5Akzk75bz5a2e2epdarvxIWfHXEHWImO4kTzJjf
WyMIDKhD77EwfognV/27HUVe43TmQtcGmwpdscwSKagoc+gC3C9IDyB+NJfVE188
zRg7Vpo38uWZnvjn87py63iCGcxSko9FPODvjmipC0zI5af25kEjzdiPIDiu+oQZ
Y5kdBVYlBkJt9KjmP4vWh+vSp+Wtu8NMYJ7jolxioKbYRdGA9tfbzKo=
-----END CERTIFICATE-----
[root@localhost CA]#
```


X509v3 Subject Key Identifier:
95:5E:C1:1B:87:E9:7C:78:0F:9A:52:18:4B:5D:7F:1C:97:82:9F:C1
X509v3 Authority Key Identifier:
keyid:7E:28:FE:CA:07:9B:5B:7D:65:75:0A:8E:8D:6A:44:F5:DD:E3:19:74
Signature Algorithm: sha256WithRSAEncryption
29:a3:44:7f:8c:da:6f:b5:ad:71:ea:e9:e7:8d:fc:81:43:b4:
a3:e7:7a:1c:26:49:31:61:09:24:f3:ab:28:e6:ee:d9:a1:f3:
78:05:7f:8e:48:05:0f:c6:f4:db:a5:79:c7:22:b5:cc:96:73:
34:72:70:58:84:92:fb:b7:d9:3c:fd:40:50:05:3d:f8:3b:a5:
f6:19:c0:d6:ca:8c:17:9f:ef:b4:5e:0c:09:e8:4b:82:ea:f3:
66:f6:56:87:8a:35:db:65:74:74:30:17:be:4d:c2:c0:97:9b:
99:e3:f0:b2:e3:fd:19:e1:cc:e6:0a:4d:b9:d3:8b:d5:d4:0e:
39:48:cb:96:4a:39:0e:08:3d:b5:de:5e:54:19:d0:b0:c4:cb:
db:18:45:32:c5:24:70:42:e0:cd:17:f5:75:90:44:f2:4e:4c:
09:66:3b:cd:6c:2e:fd:f3:61:69:69:1e:6b:71:f7:f8:e0:fb:
30:8b:de:01:17:6a:5e:ab:75:20:ef:eb:a9:d0:53:b0:65:76:
17:ac:72:8a:ab:a9:69:5f:0c:ee:0b:0d:a2:69:9d:74:78:73:
6f:e7:88:55:d8:2c:f4:40:11:c1:65:94:c8:59:ad:4a:3b:10:
73:71:01:50:a9:06:89:9a:ce:b9:de:a7:bf:2d:ab:b6:e9:b3:
7b:2a:05:ed
-----BEGIN CERTIFICATE-----
MIIEJDCCAwygAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgaAxCzAJBgNVBAYTAlVT
MRAwDgYDVQQIDAdWZXJtb250MRMwEQYDVQQHDApCdXJsaW5ndG9uMREwDwYDVQQK
DAhTa2lmZjEwMTERMA8GA1UECwwIU2tpZmYxMDExETAPBgNVBAMMCFNraWZmMTAx
MTEwLwYJKoZIhvcNAQkBFiJkYXZpZC50aG9tc2VuQG15bWFpbC5jaGFtcGxhaW4u
ZWR1MB4XDTIyMDIxNDE3MzUyOVoXDTIzMDIxNDE3MzUyOVowgYsxCzAJBgNVBAYT
AlVTMRAwDgYDVQQIDAdWZXJtb250MREwDwYDVQQKDAhTa2lmZjEwMTERMA8GA1UE
CwwIU2tpZmYxMDExETAPBgNVBAMMCFNraWZmMTAxMTEwLwYJKoZIhvcNAQkBFiJk
YXZpZC50aG9tc2VuQG15bWFpbC5jaGFtcGxhaW4uZWR1MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA0z2oEVk4kikcCBiWJd/P8JAYQWZ+qzqieAC8N1zv
O9Tpt7dDrGmbXzHTqiEKhJdJq/w4muaJPIQ4g0oSoOOD5fme5yD7EmEBMYo1moFt
dQLJRljeP1U+u8YCeFDM+PDoUj3/zUsojxsUJ+CeKi6ITw9XipdshI6OWJjTA3fN
oZCckBiiqclfIUJBqqoOBy3tItUoZ1BGxLf7VqGYiyxojUXeaJzreKoOm3UY+uoE
XXMBOPaV1qYfhx4bupALvMFRglnUZ6Uk1/6LRSyoMw5H8UenkHMGyEfi9YxdaR0C
6o0TgqmLDWfu4bemr1wzfsjdK/i3b2G7Ox5z151ROQ0f3wIDAQABo3sweTAJBgNV
HRMEAjAAMCwGCWCGSAGG+EIBDQQfFh1PcGUuU1NMIEdlbmVyYXRlZCBDZXJ0aWZp
Y2F0ZTAdBgNVHQ4EFgQUlV7BG4fpfHgPmlIYS11/HJeCn8EwHwYDVR0jBBgwFoAU
fij+ygebW31ldQqOjWpE9d3jGXQwDQYJKoZIhvcNAQELBQADggEBACmjRH+M2m+1
rXHq6eeN/IFDtKPnehwmSTFhCSTzqyjm7tmh83gFf45IBQ/G9NuleccitcyWczRy
cFiEkvu32Tz9QFAFPfg7pfYZwNbKjBef77ReDAnoS4Lq82b2VoeKNdtldHQwF75N
wsCXm5nj8LLj/RnhzOYKTbnTi9XUDjlIy5ZKOQ4IPbXeX1QZ8LDEy9sYRTLFJHBC
4M0X9XWQRPJOTAlmO81sLv3zYWlpHmtx9/jg+zCL3gEXal6rdSDv66nQU7Bldhes
coqrqWlfDO4LDaJpnXR4c2/niFXYLPRAEcFllMhZrUo7EHNxAVCpBomazrnep78t
q7bps3sqBe0=
-----END CERTIFICATE-----
[root@localhost CA]# cat websrv.crt

```
[david@localhost CA]$ cat websrv.key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIgY4WKDRYtisCAggA
MBQGCCqGSIb3DQMHBAhjypVpx5J9MgSCBMil1UVu7Ko+lDs3bMb6qyKzxzEm+63B
XFkD1u+66J8usxDCgI4gDsS12Jbz7/aQmAVB8N8rfsaYQHBQ7ATyjul4yzOB9Et2
p2ddGbeyynWxv97OZFISpfmPYlISF3ThUxVpKdk5ZTRaQxkXD17bYTm8yJjI8Z6b
Kty6oUzKCU6yfPaHaQu1r5gB5t7zyetzH750wK4UIIiLBn4BwuEVBtfmmyi3ZmzC
6kvLfzvBnmL6S3eUtR19zqJ9gZFukwbMrhqivl38GUs9HIRt4lJ1/X9AsyPFnD9b
562UcNMGh87yz5GOqIx7I6aUVarQg3CLFhpm9QlzN1B4jXKyl1jtUuni7vPVneDO
vDOYczBeFkLGVlU00vic07rBx7Vj+KgwpKa7wWMbv47HIlMVOUWYkznP9iQrkPes
68hHWEfx/sshwhNNO0tm+JjGyLYS5ayZIR+yczLvNorkVbOpTNVEevgQXg/htA13
uxmARxVEci6Hxgx4ottenm5++oXpSrKbaM8ZI2Fbb65nwFFBQt2cOgFJF1EjsD8P
PHxk91+uolES0YydGifLske5t3SXaxLr/OqciNOpEVH5HEjacy6QqegfZTRtLOP/
tOcceutW9rrGUAANlpp0p4/rartjp5JZ9L2aunJT1lSn4uPzcWnk+smij144J1H5
Bfc3KSu0WSG2pcxRZKoH7DQFLmWAJKTRwV/4FUkyJMOXgTpdZKhbrVoq7meSNxXh
blYcMD/GUyhTK9+ZsBVpNn4FT03MHr6qJBvS4KjS/WwheUgFdwerNhPY6kXlabt/
yVqgXeyUyP+EHB0hXBpK/JjjyoYcaVdk66umZTuHCG/dZvkRYeRvtCqGE2EDbSBW
0WBBeG7qnc5Che2Jg+RFiSEeX41/llzgYuD9YRyohOBX4bfThKUNuNAb8nb3luv/
xZvB5pGYABntvP176x6qIT/FgpwKPGpFKtQsLDt/q3U460G9mw5WI4txW9aTqlTx
OMBFH3HZlCByh3EyLPxWdAJOmoELQsO+sfXXbzWaX8RwThNxioiXdzqhRKiGe3Hk
G6R4GmeXf+ZWFFC+uY7lFCRsy4MLXGoDX3aHgcDhdNz4tdx10FgJrzySB9Zjc4Ti
RGW13F4AAGCdm7+F7ZAg1ZnwJErMGD1Fb9HawwicRF3Zsf7qZ4RZdvYeSyMrGVdY
kv/jWWEWlu56sgqqK4bbli28WU4j+OkXq5HYhxf3SzVYUJnmIe25ppggxmwWq9bX
aDhzcIDiHWj5u7vwUhFcvWJHjPNYDxF9w/3BAjO6JtqjsCt0ajaNmcN4IYZo94gc
YliDbUglv+oVl/Tk7jQ7o7OBdnJBUk2HH/WhgQ/GgIq1n4/9QlVV34eajXLYj4R
BVXUui4GEsfsCQxC9M2zJ8IkFJuQUOzrYUuP+uYK+0Gv6AzrudVo1vEZUWHUHVEg
6VHyt7NPd0CNmw9EuR8z74C3XA0fFkFMsKt35njLm4OgZwKr7H1L0ZHBR48DXrHu
+olstgyoV/4rQm1i4VJmnNm32Ep5MrfkD4ML0BPjjkYBC6Va0y/Ww0fam2+H4Tjk
ypXPrhxqqeQ0jNkE9rfaVCekN18SAM8LPj0CDFeCulUOsqLwEhtrmgz1XurwfUya
+Dw=
-----END ENCRYPTED PRIVATE KEY-----
[david@localhost CA]$
```