|  |  |  |
| --- | --- | --- |
| Лабораторная работа #4  «Изучение основных сетевых утилиты openssl» | Выполнил | Ноздренков С.В. |
| Группа | ЭВМ-1.Н |
| Проверил | Жариков Д.Н. |
| Подпись |  |

Цель работы: Изучить основные команды утилиты openssl.

localhost1.crt

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: sha1WithRSAEncryption

Issuer: CN=Localhost CA

Validity

Not Before: Nov 8 14:06:59 2005 GMT

Not After : Nov 6 14:06:59 2015 GMT

Subject: CN=Localhost CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:c8:db:36:d8:18:3f:93:d4:69:e4:71:cb:ad:49:

2e:a6:ec:b9:de:99:6b:53:db:59:63:1b:89:cb:b8:

3e:a5:14:58:36:4a:59:02:f6:2d:34:84:d0:31:99:

8f:45:1e:e7:62:bd:49:f4:95:ff:e2:c6:e9:41:5a:

52:66:e4:f3:a3:6e:4f:19:4a:c6:a8:34:04:59:7e:

f9:4a:3d:ac:23:4c:0b:a2:40:37:c6:cc:69:27:e6:

24:20:27:94:91:5a:d9:db:ab:90:a5:95:d4:68:76:

7d:96:f8:af:71:e7:64:cb:55:1e:c9:fe:a6:f2:4d:

a9:20:cd:77:63:c0:a0:5a:bd:7b:ec:b0:aa:9c:76:

4a:a4:d9:03:f8:d0:14:b5:b5:ce:a9:ca:58:33:d6:

84:bd:93:f0:ba:d5:86:2a:8d:ed:f2:21:85:92:e2:

43:33:69:67:db:19:ce:42:d2:7d:dc:76:23:0f:91:

10:ce:9b:a6:5e:69:aa:20:22:2c:49:78:44:5a:63:

98:4a:9d:ec:cb:38:8b:0e:f2:7e:fb:0f:51:e3:b3:

15:f2:97:0f:4f:a7:ac:d9:be:6b:be:0c:12:aa:d4:

fa:68:ec:be:67:9e:2c:c4:6d:c2:cc:69:12:3f:60:

0c:85:cd:28:06:ec:c4:ea:78:6e:75:81:b7:0a:fe:

11:53

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

8A:57:B9:8F:1E:69:2B:FA:0B:AA:2D:63:BB:85:8C:92:B4:F1:AB:A6

X509v3 Authority Key Identifier:

keyid:8A:57:B9:8F:1E:69:2B:FA:0B:AA:2D:63:BB:85:8C:92:B4:F1:AB:A6

DirName:/CN=Localhost CA

serial:00

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: sha1WithRSAEncryption

00:42:33:01:0d:61:23:3f:ce:08:95:bd:d2:6c:f6:90:c1:d8:

2f:55:fb:da:7c:7e:b3:a1:b7:b4:23:68:a5:08:9e:77:b9:27:

a7:66:5a:17:24:00:23:66:d0:44:38:7a:31:ce:48:63:0a:47:

bb:37:e2:b6:7c:8a:1b:2b:65:d3:f4:50:b5:d3:84:45:9b:10:

ff:b0:b0:55:fc:ad:8e:20:b7:0d:96:13:d9:12:c2:a4:0d:ad:

80:06:eb:3f:44:ed:f9:35:16:6d:87:9c:66:10:6c:25:59:09:

88:94:92:f9:a0:fd:a5:e2:f6:10:8d:12:51:c6:b9:57:7b:1d:

97:5b:c4:9a:ff:55:d8:37:99:46:ca:83:21:98:56:fd:a7:81:

86:27:2f:5f:a7:aa:c6:f0:c1:d9:93:53:97:ba:b8:35:a9:bc:

48:db:0e:52:8d:64:05:25:cc:5b:8d:2f:8e:3d:96:b6:6c:ca:

26:52:31:23:a0:9a:a6:76:62:43:c7:78:3c:59:c4:5b:d4:b8:

3e:cf:04:11:ba:a0:90:54:ce:1f:a7:2f:f2:65:89:5c:0b:18:

7b:0c:1f:1e:51:3e:09:a1:a7:1b:87:24:24:21:95:ce:44:83:

d2:62:ef:4d:f5:c5:30:1d:76:ed:89:6d:bf:5f:43:34:c5:f3:

f4:b3:28:a5

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

MIIDGTCCAgGgAwIBAgIBADANBgkqhkiG9w0BAQUFADAXMRUwEwYDVQQDEwxMb2Nh

bGhvc3QgQ0EwHhcNMDUxMTA4MTQwNjU5WhcNMTUxMTA2MTQwNjU5WjAXMRUwEwYD

VQQDEwxMb2NhbGhvc3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB

AQDI2zbYGD+T1GnkccutSS6m7LnemWtT21ljG4nLuD6lFFg2SlkC9i00hNAxmY9F

HudivUn0lf/ixulBWlJm5POjbk8ZSsaoNARZfvlKPawjTAuiQDfGzGkn5iQgJ5SR

Wtnbq5ClldRodn2W+K9x52TLVR7J/qbyTakgzXdjwKBavXvssKqcdkqk2QP40BS1

tc6pylgz1oS9k/C61YYqje3yIYWS4kMzaWfbGc5C0n3cdiMPkRDOm6ZeaaogIixJ

eERaY5hKnezLOIsO8n77D1HjsxXylw9Pp6zZvmu+DBKq1Ppo7L5nnizEbcLMaRI/

YAyFzSgG7MTqeG51gbcK/hFTAgMBAAGjcDBuMB0GA1UdDgQWBBSKV7mPHmkr+guq

LWO7hYyStPGrpjA/BgNVHSMEODA2gBSKV7mPHmkr+guqLWO7hYyStPGrpqEbpBkw

FzEVMBMGA1UEAxMMTG9jYWxob3N0IENBggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZI

hvcNAQEFBQADggEBAABCMwENYSM/zgiVvdJs9pDB2C9V+9p8frOht7QjaKUInne5

J6dmWhckACNm0EQ4ejHOSGMKR7s34rZ8ihsrZdP0ULXThEWbEP+wsFX8rY4gtw2W

E9kSwqQNrYAG6z9E7fk1Fm2HnGYQbCVZCYiUkvmg/aXi9hCNElHGuVd7HZdbxJr/

Vdg3mUbKgyGYVv2ngYYnL1+nqsbwwdmTU5e6uDWpvEjbDlKNZAUlzFuNL449lrZs

yiZSMSOgmqZ2YkPHeDxZxFvUuD7PBBG6oJBUzh+nL/JliVwLGHsMHx5RPgmhpxuH

JCQhlc5Eg9Ji7031xTAddu2Jbb9fQzTF8/SzKKU=

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

Здесь сертификат представлен в текстовом формате и в формате PEM.

localhost1.key

-----BEGIN RSA PRIVATE KEY-----

MIIEowIBAAKCAQEAyNs22Bg/k9Rp5HHLrUkupuy53plrU9tZYxuJy7g+pRRYNkpZ

AvYtNITQMZmPRR7nYr1J9JX/4sbpQVpSZuTzo25PGUrGqDQEWX75Sj2sI0wLokA3

xsxpJ+YkICeUkVrZ26uQpZXUaHZ9lvivcedky1Ueyf6m8k2pIM13Y8CgWr177LCq

nHZKpNkD+NAUtbXOqcpYM9aEvZPwutWGKo3t8iGFkuJDM2ln2xnOQtJ93HYjD5EQ

zpumXmmqICIsSXhEWmOYSp3syziLDvJ++w9R47MV8pcPT6es2b5rvgwSqtT6aOy+

Z54sxG3CzGkSP2AMhc0oBuzE6nhudYG3Cv4RUwIDAQABAoIBAQCARF3VykZvpWqq

VHF5jA6a0vovyVHdD2sZ+3AYBOUcjs12fiwx0/wyWc6KnkH8JiwlxjQAWfo7XEOB

VKjixLtCVyN0R2ht6ioM7SVN3+yZ7epQByqXbdqJfFL9pckeuiH+QqXw2Kn4vBKf

4thHqTmZEBbFcDY07ptfM1dXAKBm0REvYUKaFVbmmjvcfaYNjLjxnK7NvyLT7FnK

E9rrtFBWVYP+wBNPpRx4L1RcpSBIH1xyQY4U9urJCrJKUNg/qatYYnm2/d5XDY4+

FGzr2OcfovCtLkOtGy/L1SBZ272bNL7c1V2xsTDfQtjV3ZtEeyEc6XXW0s30PrEV

eePDM1vBAoGBAOeXPq0+a2q6+epbQRH+TOaRwc+4V5A6dyISc/RE6sF/FRiuYjbN

vRxkG6J49UA7i+eEURRYUn3oWkvOkybsK305ACBXMtlDibGM65yQuha6QsHA0JoA

rnivrWe5nP+RewPyOlb3zCPYOnqrUPwQBL+3uRKdaC9WsmLzgmJ/VU2pAoGBAN4G

sekKBceLa9g49wFHHOu5p0xNgp8m5poco5nHNHWdUQReAPQN1VNV11BXtzzQQtll

b5jjxS8ExJnRCbVHwc92Duvw08miLnyoQLTbF0lZesyF8uKn965ohofHfFCK46B5

8xqwZWjOhfruVZDTfgJZ5ICsrSVmrTokJcj6ZyybAoGAbMaPO9P7pA/aXocqEwd8

mzeO7r/I8Qdk+W3tZKgSE3xbLlKJ8u/DiVhD2pYxq0/MsJtnccTiSh0efEi0uS1o

Z9KkCoyqZ33faLOl3s3jedVWkaa80/jJ+gmZywRVh3yPaRUW7c5J5fQj04Yv7ZSg

hmQG24Vvb/yqoOt7LERejrECgYAHR8brslVwLqUxqOSImTFclXDj8qK230qugQPo

VfzlYmw2rXJwjkeRfP4bd1Td3KJkiIv5QnbDzO85b/5WgGzdhayFlhcLxJKrqcS9

aXXBBPse28GUJxfbEzheGW99IKDIMVeEZ4ZbwnHoQYpyvkyifRoeEgt3b398qZTH

m1ZowwKBgEOtUt7S4MIWlsM7lSKd20dYNdctx8Vnbty6wqFmRQ21M55SQFF/zw+j

0CY9Syc9S4lDbp71jY7Z3LCJABFizZucROAzXm7Iut06+8pakqVCqV0g7AIEeAeU

gL8hJ/QCvBVsf3MNMC8FmUf8LTTyBxIvA4U3KjGjmxaHMLh+TloT

-----END RSA PRIVATE KEY-----

Закрытый ключ представлен в формате PEM.