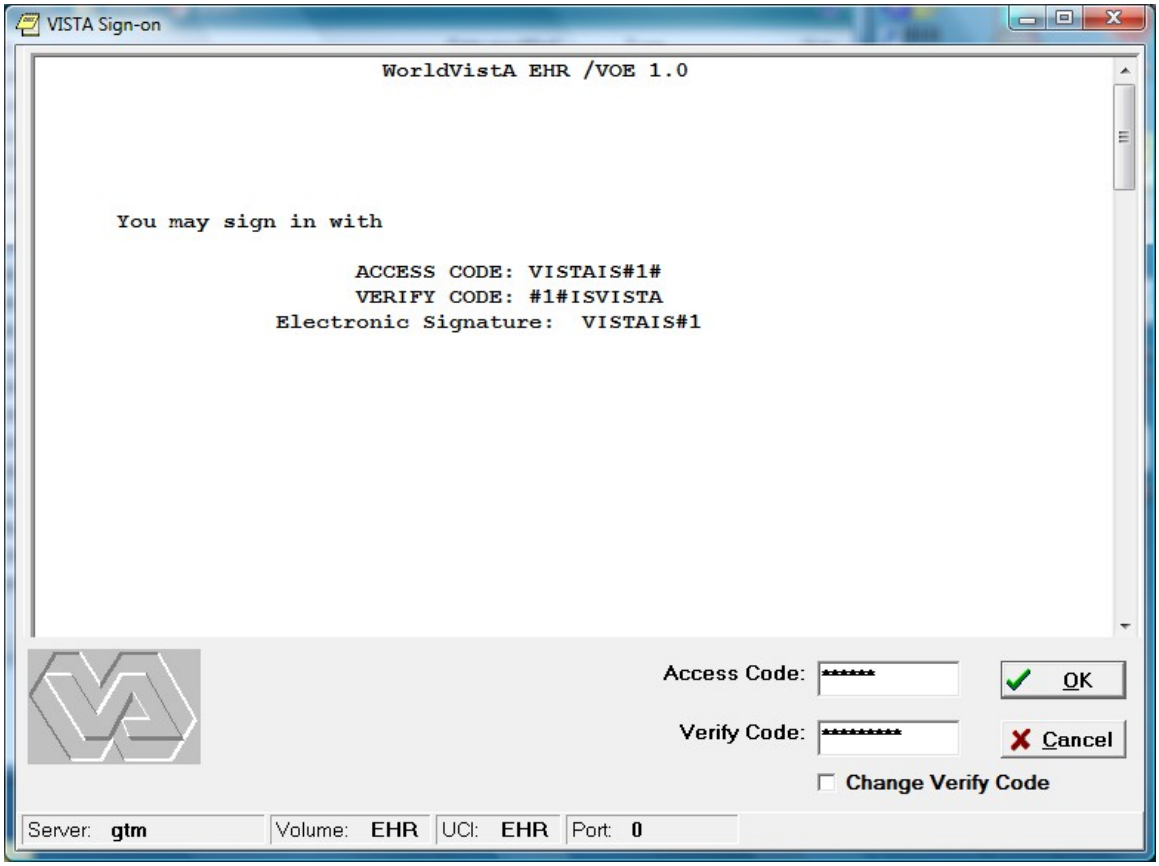
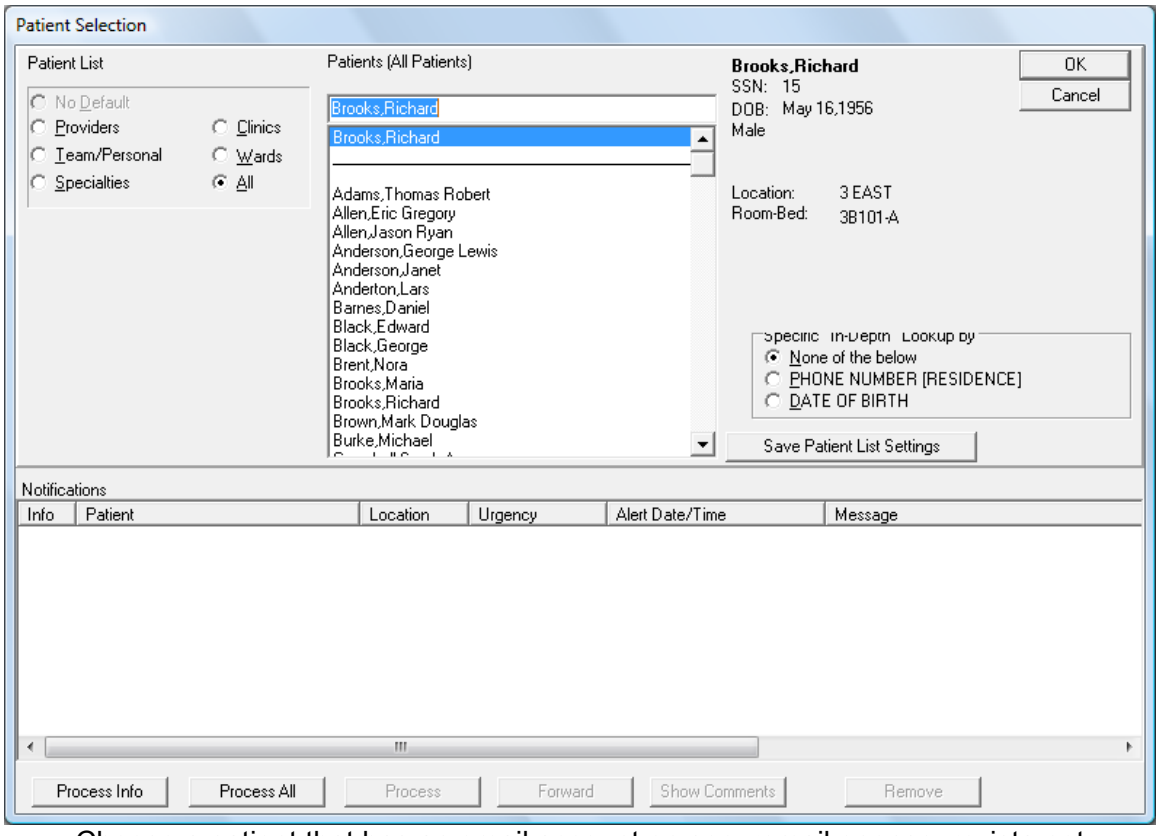
Requirement	*RequirementSatisfied (Yes/No)*	*Vendor Response/Submission/Comments*
§170.302.v: Encryption when exchanging electronic health information		
Provide EHR documentation that specifies encryption and decryption capabilities and identifies algorithm and encryption key specifications used.		Provide details about when encryption/decryption is used, algorithms used, and key specifications.
Provide unique test data elements to be used for the testing of this module only.		
Provide identification of the technology used to transmit electronic health information over an encrypted and integrity protected link. Note: This Test Procedure does not require the use of any particular technology or algorithms, nor does it dictate when an encrypted and integrity protected link must be used for specific types of data. The conditions under which the link is used is determined by the user.		Provide details of the transmission technology.
Provide a declaration of the external system to be used for the testing of this module. 1) The external system can either be a receiving system specified by InfoGard which is configurable to use the transport technology of the EHR, or a vendor-identified system capable of receiving from the EHR. 2) If the InfoGard specified system is used, the vendor must provide the communication configuration information necessary for transmission. 3) If the vendor-identified system is used, the vendor must provide a description of how to configure and use the system.		Provide a description of the external system to be used for the testing of this module and the configuration information necessary.
Provide instructions on how to use the EHR functions to: 1) Encrypt electronic health information. 2) Decrypt electronic health information. 3) Transmit electronic health information to an external receiving system using the Vendor-identified encrypted and integrity protected link.		All functions listed must be tested.

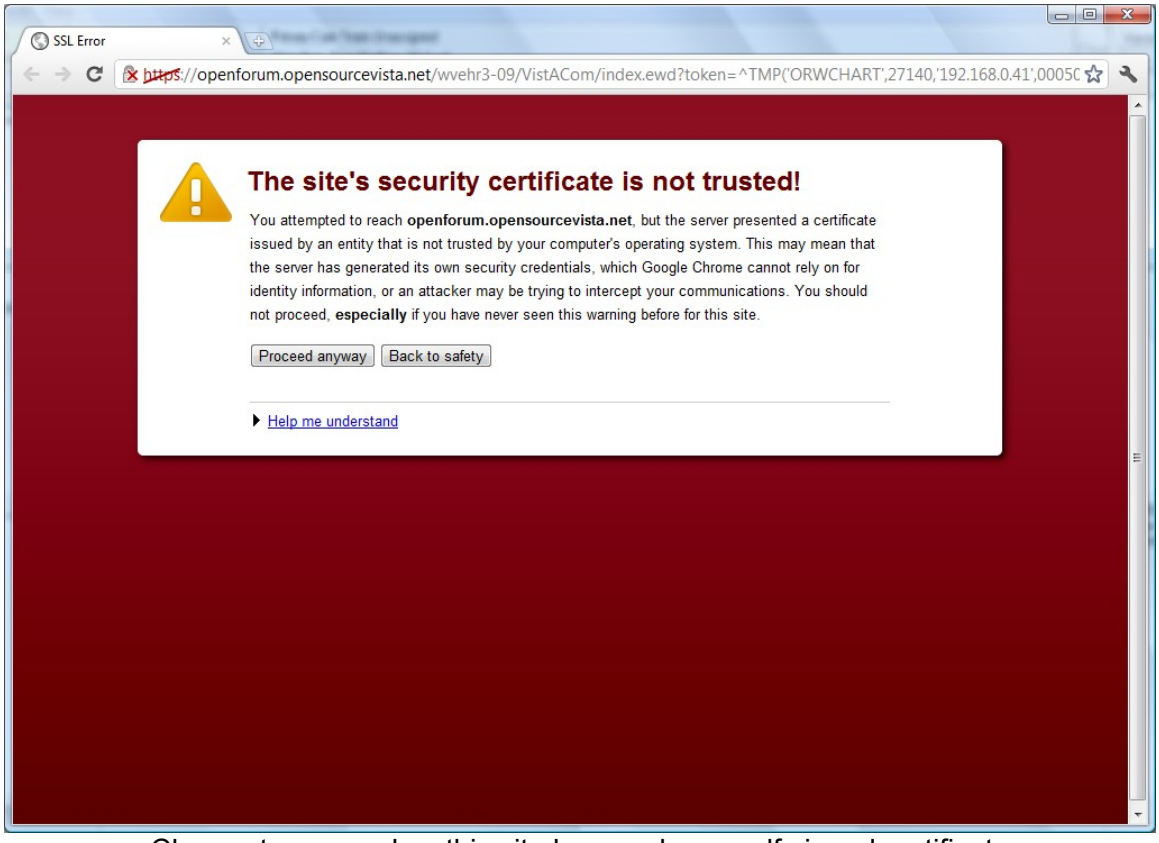
WorldVistA EHR System Provider Sending Encrypted Health Information Securely



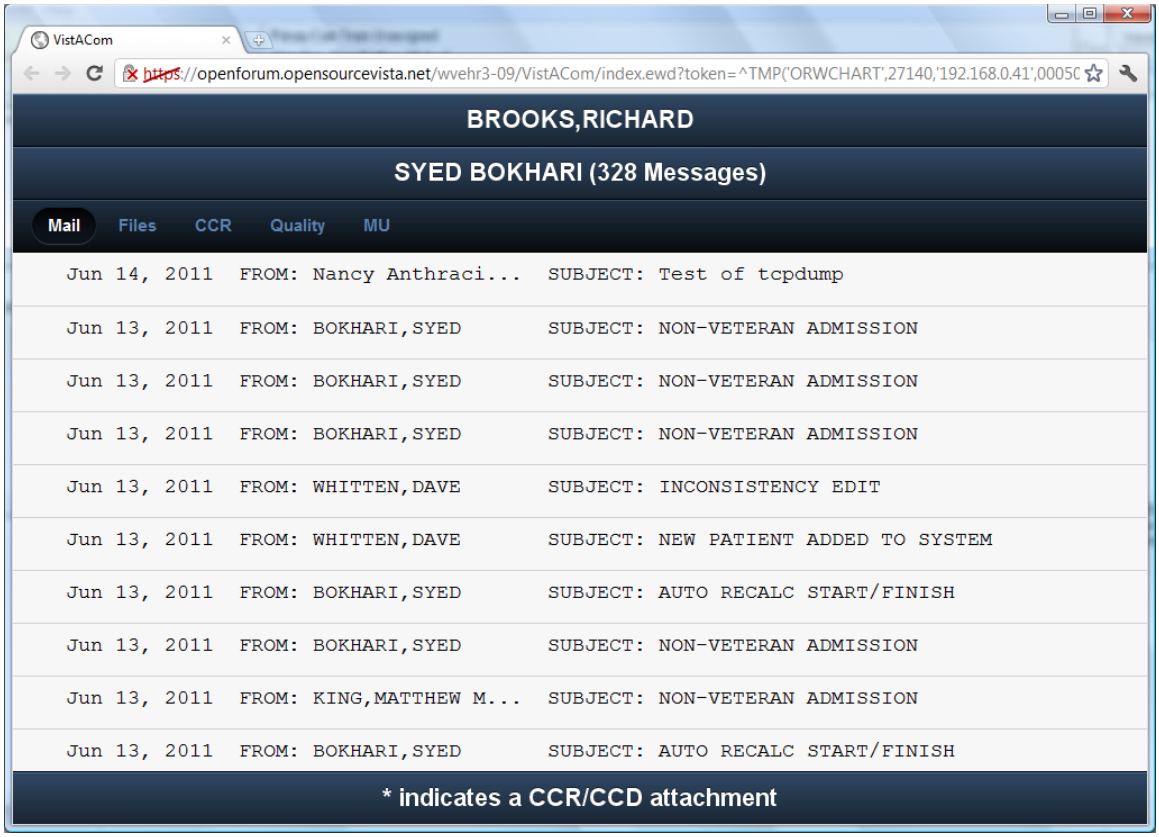
Log Into CPRS



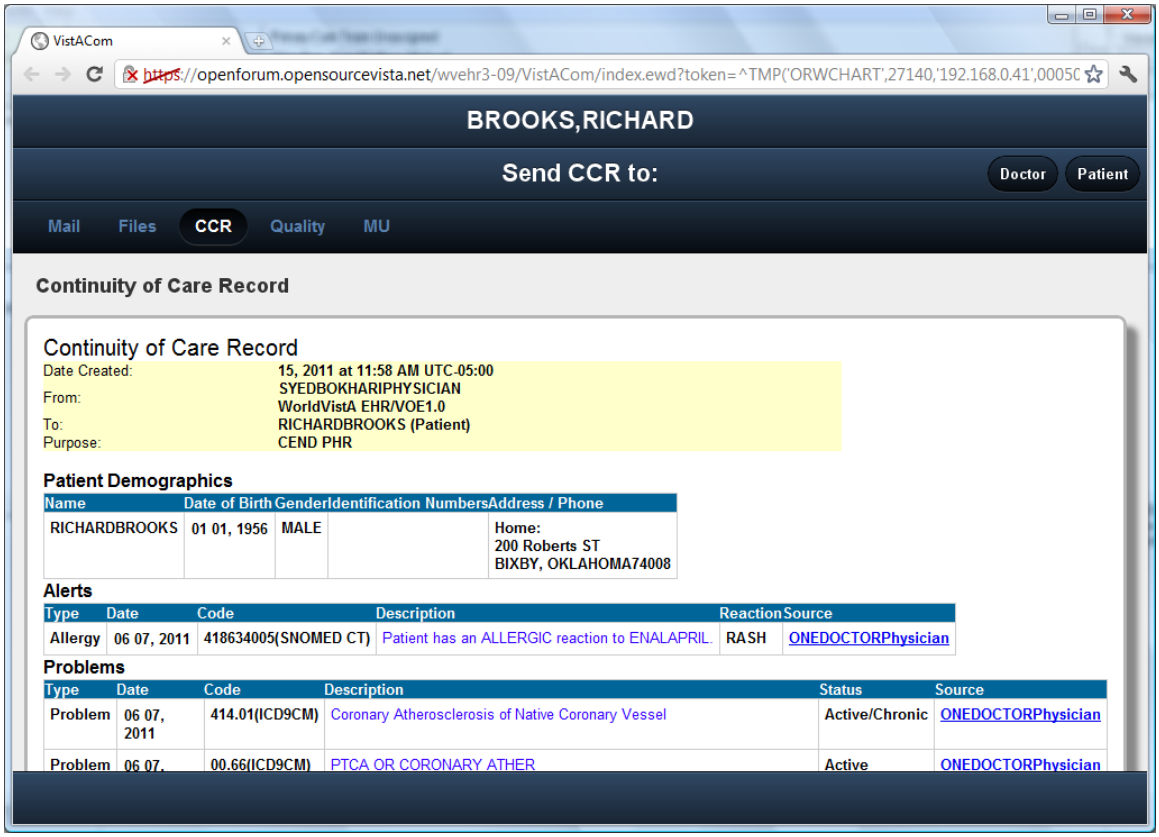
Choose a patient that has an email account on securemail.opensourcvista.net



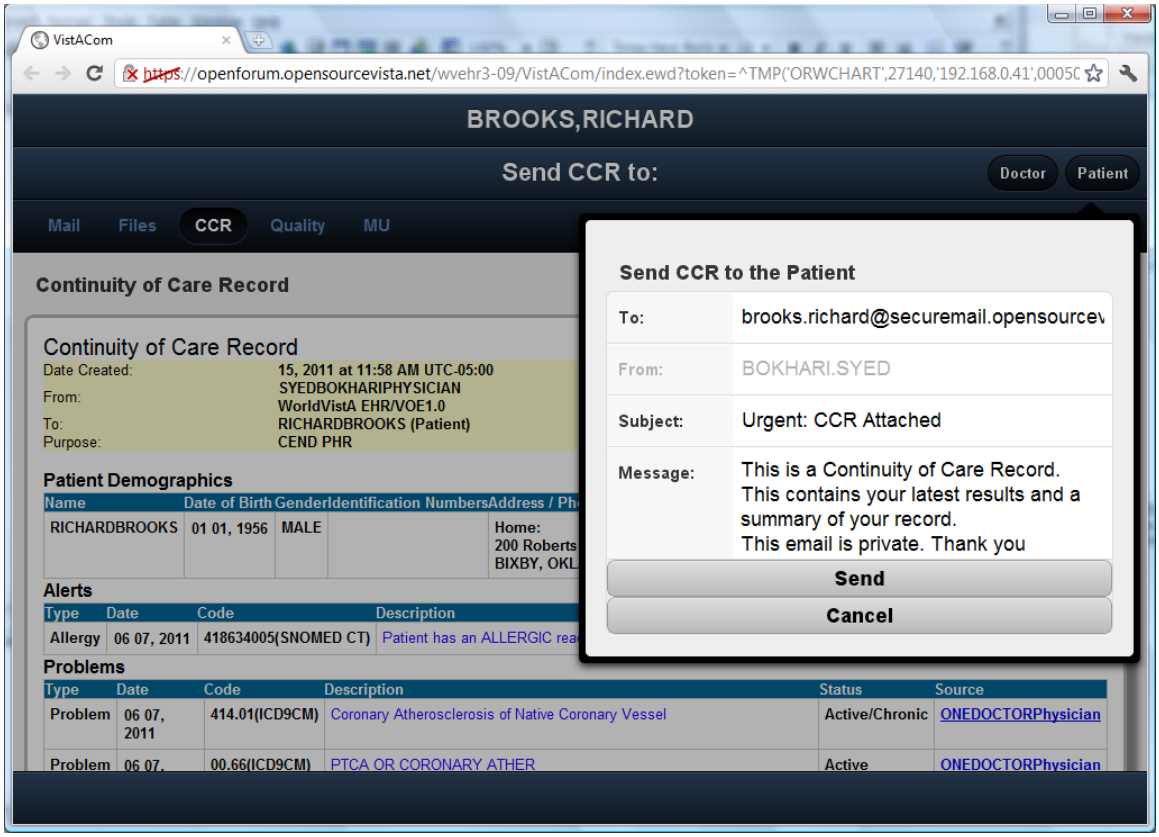
Choose to proceed as this site has our know self signed certificate



This will take you to the page listing all of the emails for you . Click on the third item over in the toolbar, i.e. CCR.

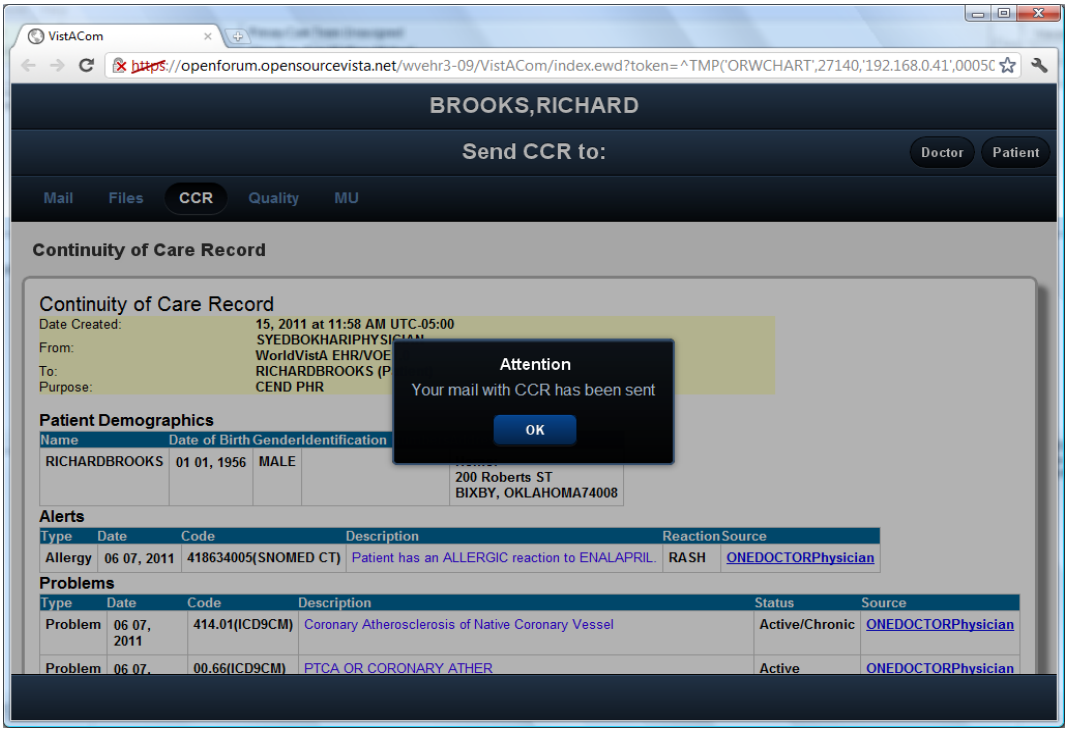


The latest CCR is displayed in real time. Click on the button in the upper right hand corner that says “Patient”.

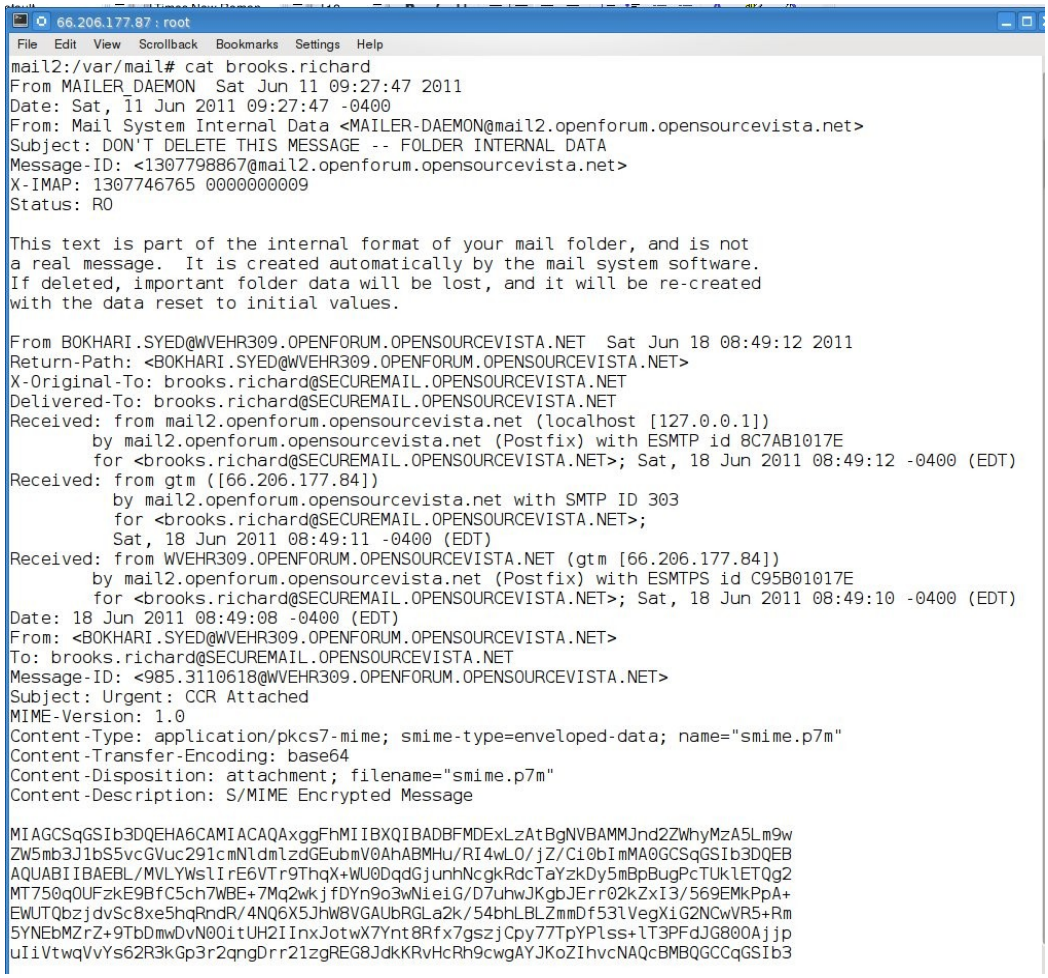


Address the email to the patient in at the securemail.opensourcevista.net which will send the email to a pop3 server which will deliver the message encrypted and signed to be picked up by the patient. The email is delivered to the patient only with a login, certificates present and with the use

of StartTLS and when the patient picks up his email, the event is logged.



Notification that the Email is sent.

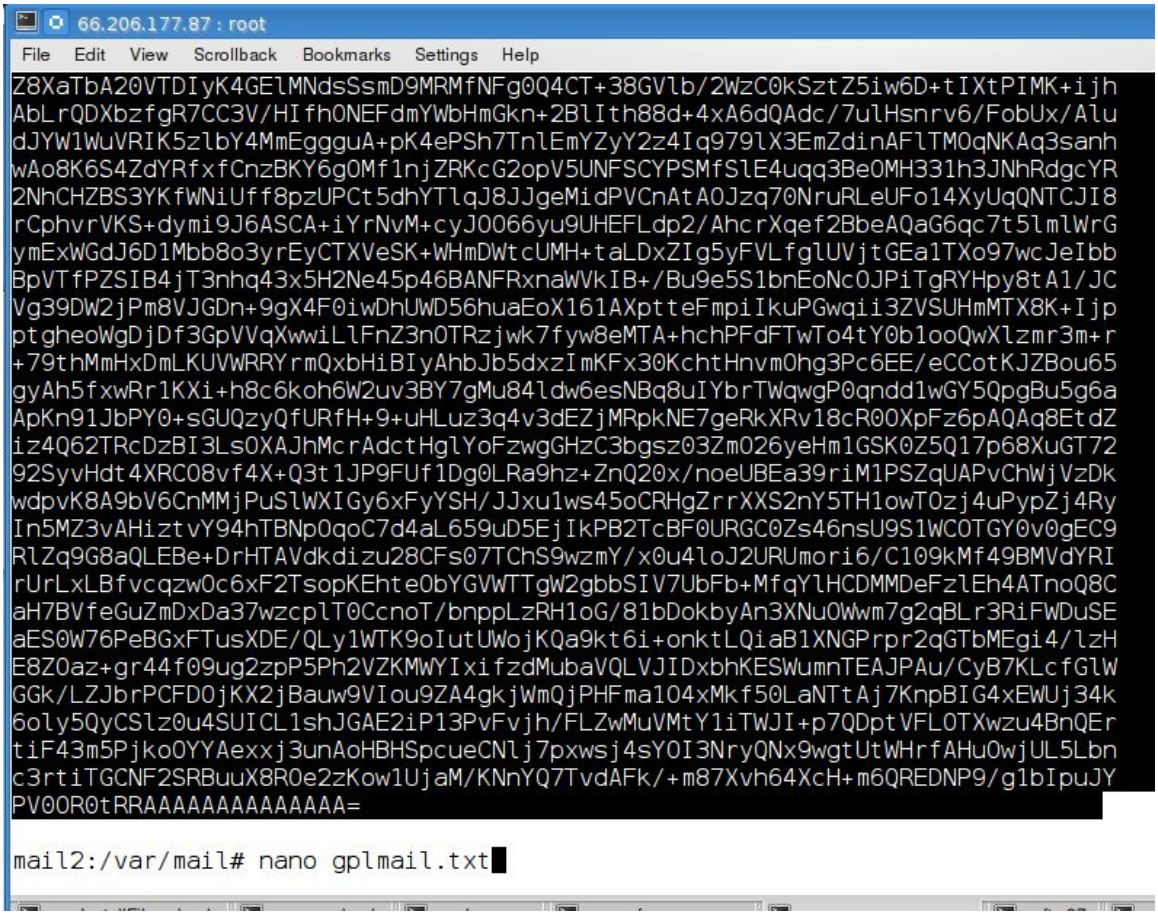


Email is encrypted and signed and stored by the Dovecot POP3 server on the local system awaiting pickup with a TLS encrypted link to a mail client capable of handling StartTLS and keys for decrypting. The mail is stored in /var/mail/[Large File Named For the Intended Email Recipient]

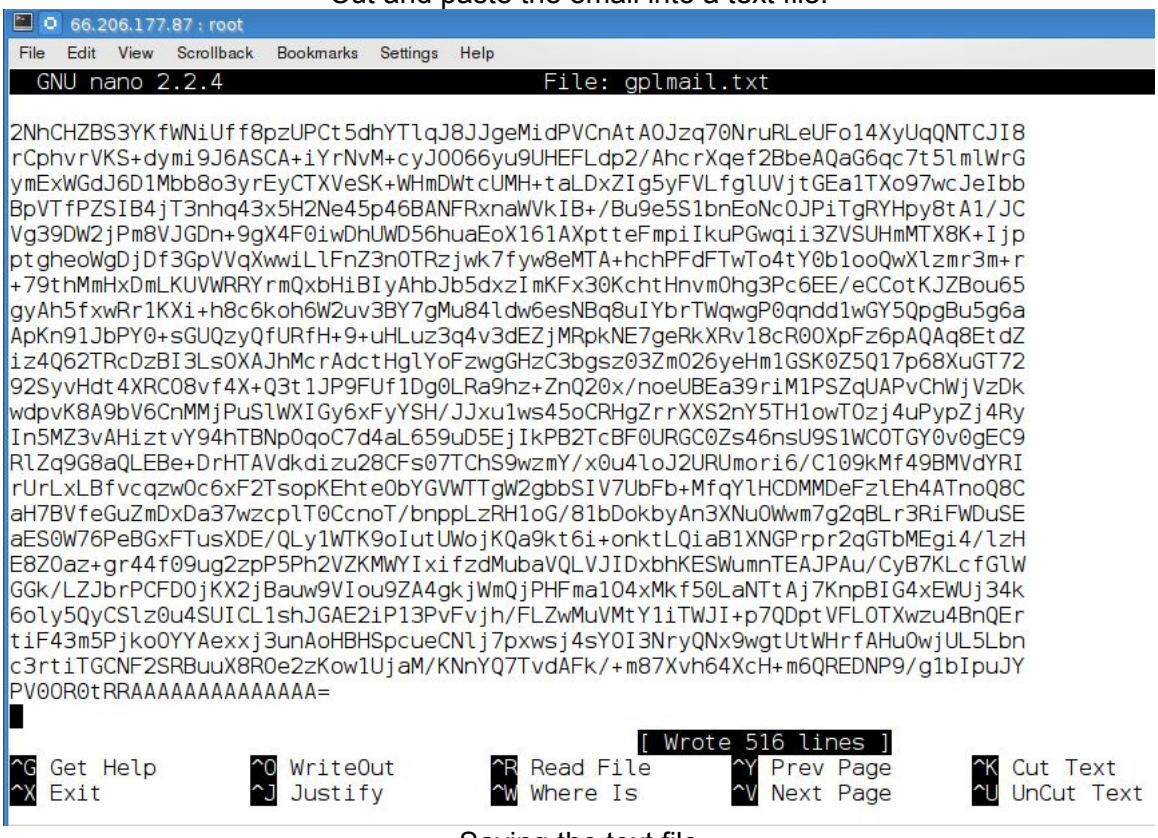
S/MIME encryption is a two level process. The message is encrypted with a secret key (aka session key) and the session key is encrypted with the public key of the recipient.

By default the secret key encryption algorithm is 3DES. This can be changed to AES if required. The reason why 3DES was choses for the default is that Windows XP only supports AES since service pack 3 (SP3).

The public key encryption is done with RSA. The encryption strength of the public key encryption is determined by the length of the public key. In this case it is 2048 bits. The encryption of outgoing email an decryption of incoming email is done by Djigzo.



Cut and paste the email into a text file.



Saving the text file

openssl pkcs12 -in brooks.richardATsecuremail.pfx > brooks.richardATsecuremail.pem

User key ise uploaded and converted to the proper format for decrypting email with OpenSSL.

openssl smime -decrypt -in gplmail.txt -inkey brooks.richardATsecuremail.pem
Email is decrypted using openssl. This format is 64 bit mime encoding that is not encrypted.

Capture of the decryption process and the decrypted mail

mail2:~/smime# ls
brooks.richardATsecuremail.pfx gplmail.txt
mail2:~/smime# **openssl pkcs12 -in brooks.richardATsecuremail.pfx > brooks.richardATsecuremail.pem**
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
mail2:~/smime# ls
brooks.richardATsecuremail.pem brooks.richardATsecuremail.pfx gplmail.txt
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
mail2:~/smime# ls
brooks.richardATsecuremail.pem brooks.richardATsecuremail.pfx gplmail.txt
mail2:~/smime# **openssl smime -decrypt -in gplmail.txt -inkey brooks.richardATsecuremail.pem >> gplmaildecrypted.txt**
Enter pass phrase for brooks.richardATsecuremail.pem:
mail2:~/smime# ls -l
total 84
-rw-r--r-- 1 root root 6881 Jun 21 00:19 brooks.richardATsecuremail.pem
-rw-r--r-- 1 root root 5281 Jun 20 17:43 brooks.richardATsecuremail.pfx
-rw-r--r-- 1 root root 27183 Jun 21 00:20 gplmaildecrypted.txt
-rw-r--r-- 1 root mail 39020 Jun 21 00:01 gplmail.txt
mail2:~/smime# **cat gplmaildecrypted.txt**
Subject: Urgent: CCR Attached
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1;
	boundary="----=_Part_1174_12039370.1308622124861"

------=_Part_1174_12039370.1308622124861
Subject: Urgent: CCR Attached
Content-type: multipart/mixed; boundary=123456899999

--123456899999
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit

This is a Continuity of Care Record.
This email is private. Thank you

--123456899999
Content-Type: text/xml; name=ccr.xml
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=ccr.xml

PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGL
TgiPz48P3htbC1zdHlsZXNoZWV0IHR5cGU9InRleHQveH
NsIiBocmVmPSJjY3IueHNsIj8+PENvbnRpbnVpdHlPZkN
hcmVSZWNvcmQgeG1sbnM9InVybjphc3RtLW9yZzpDQ1Ii
PjxDQ1JEb2N1bWVudE9iamVjdElEPmI2YjkzMmNlLWYzO
DItNGMyYi1hY2NlLTJkZDA5MTdiMDYzNTwvQ0NSRG9jdW
1lbnRPYmplY3RJRD48TGFuZ3VhZ2U+PFRleHQ+RW5nbGl

zaDwvVGV4dD48L0xhbmd1YWdlPjxWZXJzaW9uPlYxLjA8
L1ZlcnNpb24+PERhdGVUaW1lPjxFeGFjdERhdGVUaW1lP
jIwMTEtMDYtMjBUMjI6MDc6MDUtMDQ6MDA8L0V4YWN0RG
F0ZVRpbWU+PC9EYXRlVGltZT48UGF0aWVudD48QWN0b3J

//SNIP

Now show that the text above is meerly base64 encoded, clip out that section and put it in a text file and decode that.

nano ccr.xml.base64
base64 -d ccr.xml.base64

mail2:~/smime# nano ccr.xml
mail2:~/smime# base64 -d ccr.xml.base64
<?xml version="1.0" encoding="UTF-8"?><?xml-stylesheet type="text/xsl" href="ccr.xsl"?><ContinuityOfCareRecord xmlns="urn:astm-org:CCR"><CCRDocumentObjectID>b6b932ce-f382-4c2b-acce-2dd0917b0635</CCRDocumentObjectID><Language><Text>English</Text></Language><Version>V1.0</Version><DateTime><ExactDateTime>2011-06-20T22:07:05-04:00</ExactDateTime></DateTime><Patient><ActorID>ACTORPATIENT_15</ActorID></Patient><From><ActorLink><ActorID>ACTORPROVIDER_77</ActorID></ActorLink><ActorLink><ActorID>ACTORSYSTEM_1</ActorID></ActorLink></From><To><ActorLink><ActorID>ACTORPATIENT_15</ActorID><ActorRole><Text>Patient</Text></ActorRole></ActorLink></To><Purpose><Description><Text>CEND PHR</Text></Description></Purpose><Body><Problems><Problem><CCRDataObjectID>PROBLEM1</CCRDataObjectID><DateTime><ExactDateTime>2011-06-07T00:00:00-04:00</ExactDateTime></DateTime><Type><Text>Problem</Text></Type><Description><Text>Coronary Atherosclerosis of Native Coronary Vessel</Text><Code><Value>414.01</Value><CodingSystem>ICD9CM</CodingSystem></Code></Description><Status><Text>Active/Chronic</Text></Status><Source><Actor><ActorID>ACTORPROVIDER_11</ActorID></Actor></Source></Problem><Problem><CCRDataObjectID>PROBLEM2</CCRDataObjectID><DateTime><ExactDateTime>2011-06-07T00:00:00-04:00</ExactDateTime></DateTime><Type><Text>Problem</Text></Type><Description><Text>PTCA OR CORONARY ATHER</Text><Code><Value>00.66</Value><CodingSystem>ICD9CM</CodingSystem></Code></Description><Status><Text>Active</Text></Status><Source><Actor><ActorID>ACTORPROVIDER_11</ActorID></Actor></Source></Problem><Problem><CCRDataObjectID>PROBLEM3</CCRDataObjectID><DateTime><ExactDateTime>2011-06-20T00:00:00-04:00</ExactDateTime></DateTime><Type><Text>Problem</Text></Type><Description><Text>Old Myocardial Infarction</Text>
//SNIP

Now to display the ceritificates from the blob signature

openssl pkcs7 -in signature.bin -inform DER -text -print_certs

~/smime# openssl pkcs7 -in signature.bin -inform DER -text -print_certs

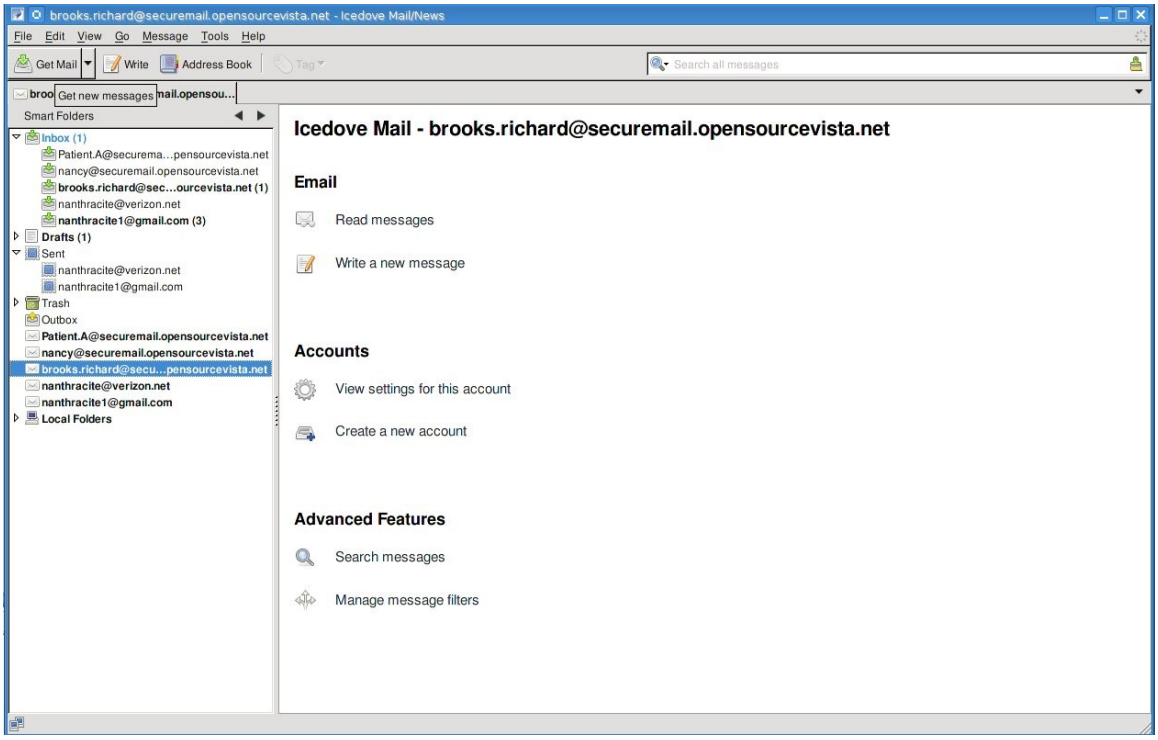
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:30:7b:12:67:c7:7f:04:08:b9:7a:7e:0e:eb:f0:9a
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=wvehr309.openforum.opensourcevista.net
        Validity
            Not Before: Jun  9 19:41:01 2011 GMT
            Not After : Jun  8 19:41:01 2016 GMT
        Subject: O=WorldVistA, CN=lilly.george@wvehr309.openforum.opensourcevista.net, SN=Lilly,
GN=George/emailAddress=lilly.george@wvehr309.openforum.opensourcevista.net
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:bb:95:ee:28:8a:c7:6a:f1:df:cb:12:f8:1a:83:
                    e9:6d:18:fe:b7:e0:16:4b:c4:c7:f2:53:0a:34:02:
                    58:22:8c:48:b8:c5:bb:4e:18:67:3f:06:08:d6:fa:
                    ba:40:f8:5f:bd:6f:83:28:b6:0a:16:bb:4d:5a:52:
                    35:9b:b7:32:d3:91:01:c3:6c:de:6d:cb:c7:49:00:
                    98:cf:23:4e:2f:f7:2f:99:c8:74:56:a5:4c:b5:d8:
                    63:76:01:0d:46:45:93:77:7c:06:cc:bc:4c:a9:f2:
                    36:c9:eb:e2:46:f3:71:a4:93:9a:8c:8e:04:53:71:
                    83:63:2f:ca:3b:c2:1f:f3:94:4e:5a:20:06:ab:3d:
                    94:cf:f0:e0:72:04:31:0c:68:f2:2d:49:fa:53:60:
                    0d:00:3a:3f:65:62:01:e0:4d:da:71:8a:d4:4a:a1:
                    6b:1c:af:d6:07:f2:5e:09:bf:72:2c:0b:f6:c6:fa:
                    e1:44:1e:e4:4f:1c:62:c3:85:bb:1c:86:85:b6:c9:
                    93:67:e7:56:39:b6:1d:ab:b1:5e:3b:84:23:08:42:
                    55:28:9c:57:98:e0:6d:00:41:3f:a3:c8:19:3a:77:
                    1a:87:0f:4d:29:79:f0:67:89:46:08:10:c9:ab:71:
                    db:65:6e:a5:dc:85:67:42:fa:6a:df:61:a9:b9:ec:
                    ef:23
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                email:lilly.george@wvehr309.openforum.opensourcevista.net
            X509v3 Subject Key Identifier:
                4E:7F:2E:45:0D:0B:4C:49:CC:0D:62:D7:DE:A9:1F:30:CC:F8:9A:84
            X509v3 Authority Key Identifier:
                keyid:38:A4:60:18:35:CB:C1:BE:D5:BB:5F:7E:78:72:E0:32:60:5C:1F:7F
                DirName:/CN=noot wvehr309.openforum.opensourcevista.net
                serial:01:30:2E:E2:1C:6F:3D:44:77:71:BE:E0:B0:BD:13:67

    Signature Algorithm: sha1WithRSAEncryption
        00:35:af:5d:73:b4:4e:2d:ca:44:19:eb:d4:4f:0c:b2:7c:62:
        3e:3a:91:69:8e:d1:fa:f2:5f:d4:32:c1:ad:84:22:f1:c9:b9:
        80:a4:00:bf:17:46:d3:10:ac:1b:31:22:71:16:25:9c:ca:05:
        8d:1c:fb:65:f0:ac:e7:6d:91:e3:ea:10:8f:f0:dd:97:9e:e2:
        fb:da:61:b6:86:fe:de:7f:c0:bb:a9:83:f1:31:98:57:26:54:
        a4:88:06:a2:8b:c7:4e:71:a5:ff:91:6d:07:1a:08:e6:c5:c5:
        1b:4c:90:8f:64:8f:61:54:e6:7a:9b:66:39:0a:27:a5:87:41:
        2b:06:48:0a:d3:4c:61:8d:9c:a8:87:72:05:75:ac:3f:5c:b4:
        e8:f9:1e:10:ae:80:ab:ac:98:fc:9a:ec:76:05:e9:3f:b1:2d:
        76:20:27:e3:7e:2e:72:b2:c5:64:45:29:8f:b5:24:8f:7a:9c:
        ed:8e:15:fc:37:20:34:91:8a:41:48:e6:d3:c2:21:bb:25:bc:
        cd:d8:7a:87:83:ea:d9:74:3b:0a:a3:ad:e4:98:1d:45:48:1b:
        bd:f2:dc:03:6b:71:4d:ee:33:c2:63:56:79:44:21:85:2f:f7:
        2e:cb:86:83:5c:c0:c4:78:cf:6f:fe:5e:fb:14:f3:2f:d8:96:
        4b:63:d9:ff
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIQATB7EmfHfwQIuXp+DuvwmjANBgkqhkiG9w0BAQUFADAx
MS8wLQYDVQQDDCZ3dmVocjMwOS5vcGVuZm9ydW0ub3BlbnNvdXJjZXZpc3RhLm5l
dDAeFw0xMTA2MDkxOTQxMDFaFw0xNjA2MDgxOTQxMDFaMIG4MRMwEQYDVQQKDApX
b3JsZFZpc3RBMTwwOgYDVQQDDDNsaWxseS5nZW9yZ2VAd3ZlaHIzMDkub3BlbmZv
```

cnVtLm9wZW5zb3VyY2V2aXN0YS5uZXQxDjAMBgNVBAQMBUxpbGx5MQ8wDQYDVQQq
//Snip

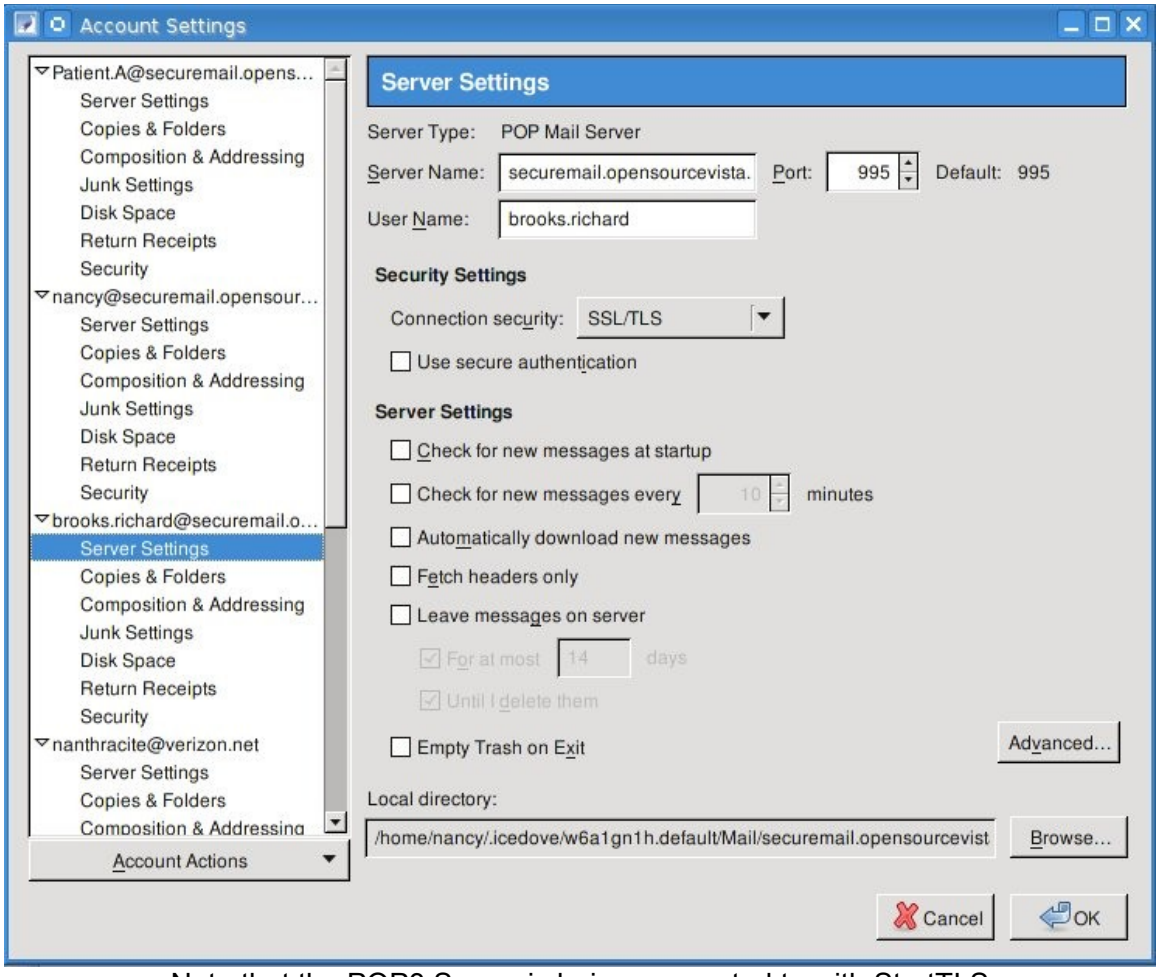
and to the display the binary content at the end

openssl asn1parse -in signature.bin -inform DER

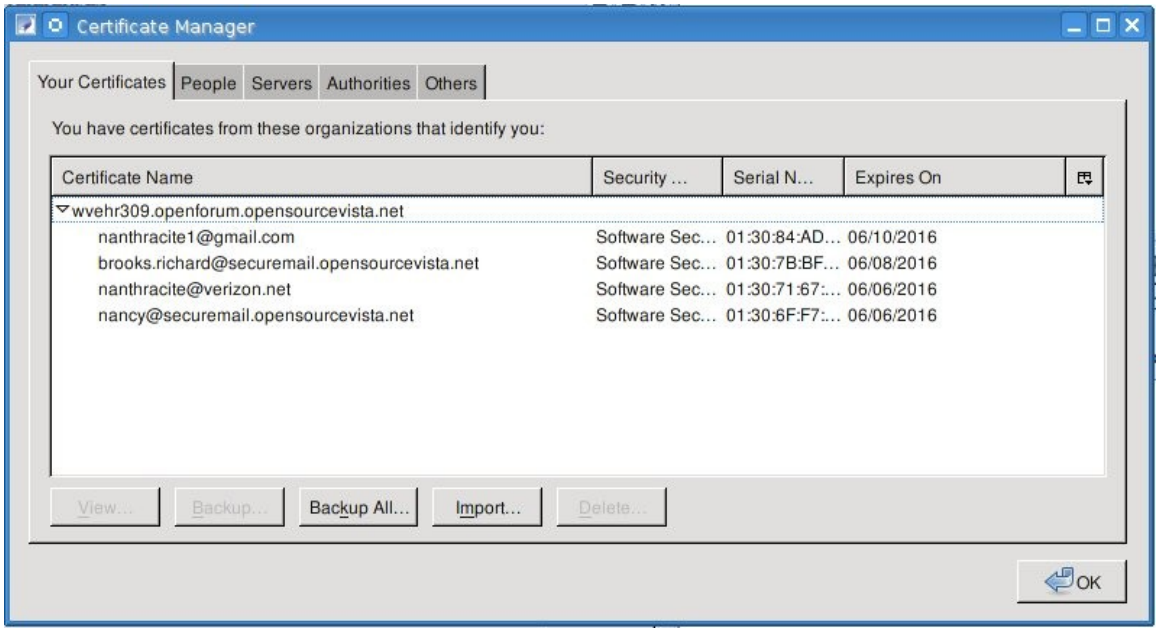
```
mail2:~/smime# openssl asn1parse -in signature.bin -inform DER
    0:d=0  hl=2 l=inf  cons: SEQUENCE
    2:d=1  hl=2 l=   9 prim: OBJECT            :pkcs7-signedData
   13:d=1  hl=2 l=inf  cons: cont [ 0 ]
   15:d=2  hl=2 l=inf  cons: SEQUENCE
   17:d=3  hl=2 l=   1 prim: INTEGER           :01
   20:d=3  hl=2 l=  11 cons: SET
   22:d=4  hl=2 l=   9 cons: SEQUENCE
   24:d=5  hl=2 l=   5 prim: OBJECT            :sha1
   31:d=5  hl=2 l=   0 prim: NULL
   33:d=3  hl=2 l=inf  cons: SEQUENCE
   35:d=4  hl=2 l=   9 prim: OBJECT            :pkcs7-data
   46:d=4  hl=2 l=   0 prim: EOC
   48:d=3  hl=2 l=inf  cons: cont [ 0 ]
   50:d=4  hl=4 l=1142 cons: SEQUENCE
   54:d=5  hl=4 l= 862 cons: SEQUENCE
   58:d=6  hl=2 l=   3 cons: cont [ 0 ]
   60:d=7  hl=2 l=   1 prim: INTEGER           :02
   63:d=6  hl=2 l=  16 prim: INTEGER           :
01307B1267C77F0408B97A7E0EEBF09A
   81:d=6  hl=2 l=  13 cons: SEQUENCE
   83:d=7  hl=2 l=   9 prim: OBJECT            :sha1WithRSAEncryption
   94:d=7  hl=2 l=   0 prim: NULL
   96:d=6  hl=2 l=  49 cons: SEQUENCE
   98:d=7  hl=2 l=  47 cons: SET
  100:d=8  hl=2 l=  45 cons: SEQUENCE
  102:d=9  hl=2 l=   3 prim: OBJECT            :commonName
  107:d=9  hl=2 l=  38 prim: UTF8STRING
:wvehr309.openforum.opensourcevista.net

//SNIP
```



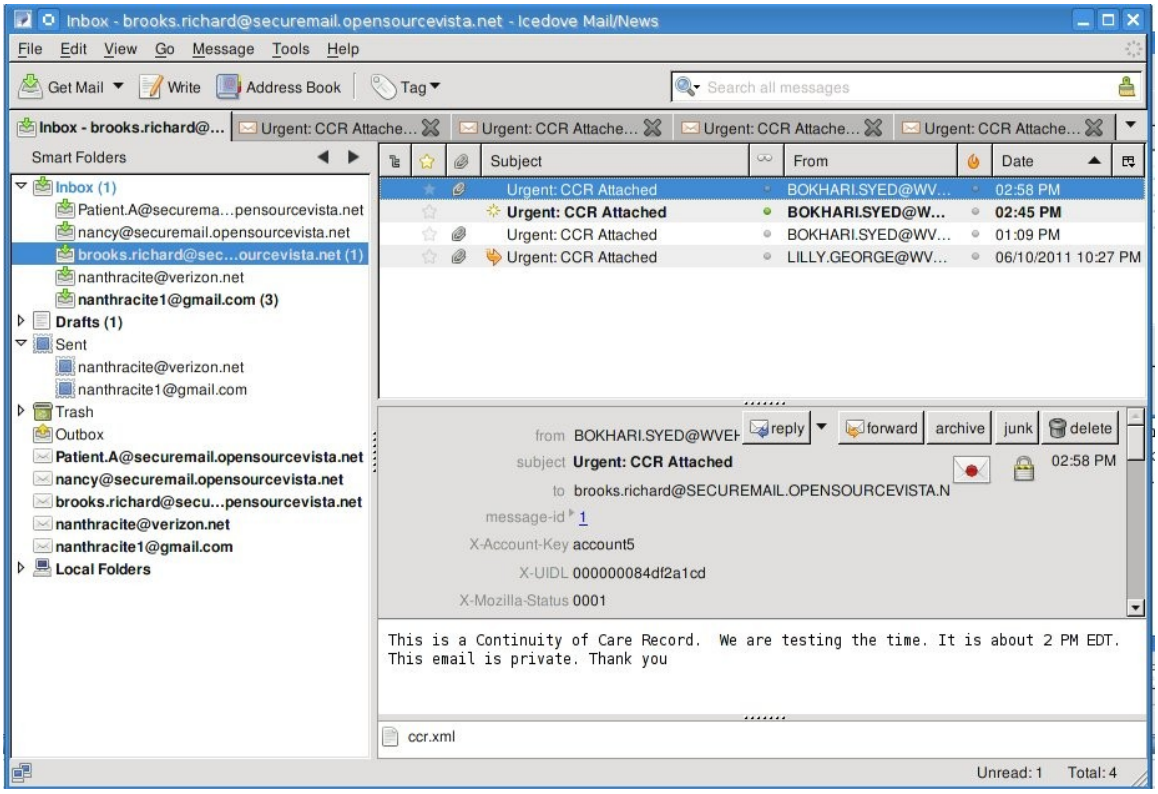
Now the email is actually transmitted by hignlighting the properly setup account of Richard Brooks and click on Get Mail.



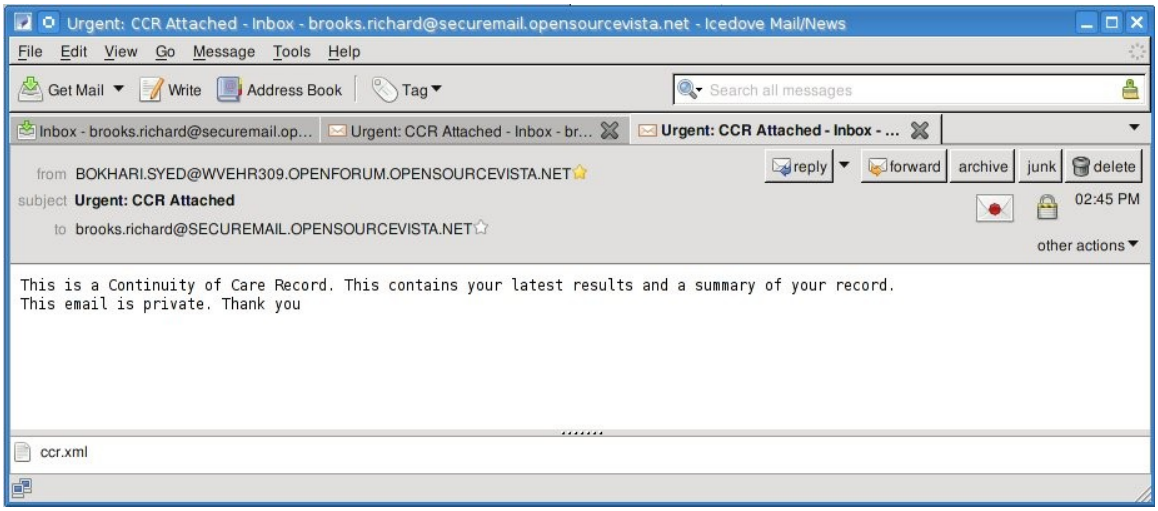
Note that the POP3 Server is being connected to with StartTLS



Note that Certificates Are Present from the source for the brooks.richard@securemail.opensourcevista.net account and Richard's certificates are likewise present on the mail server.



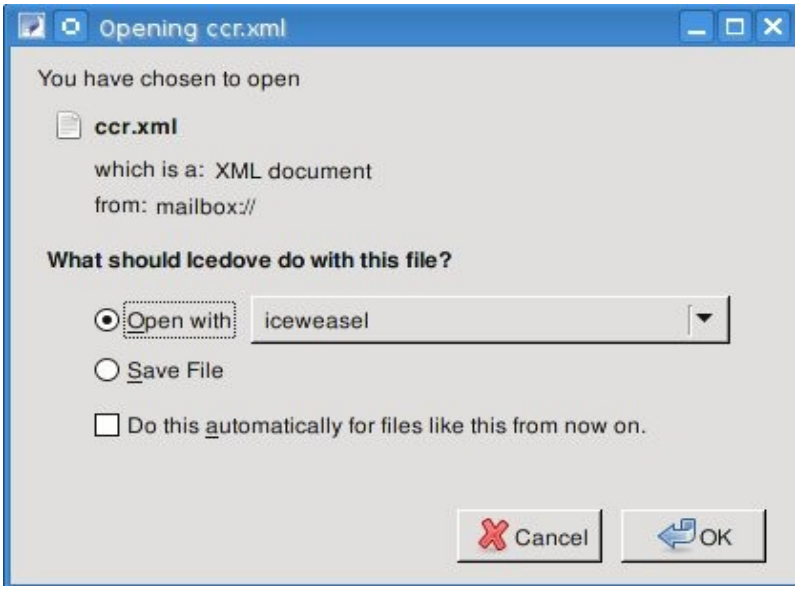
Email is received.



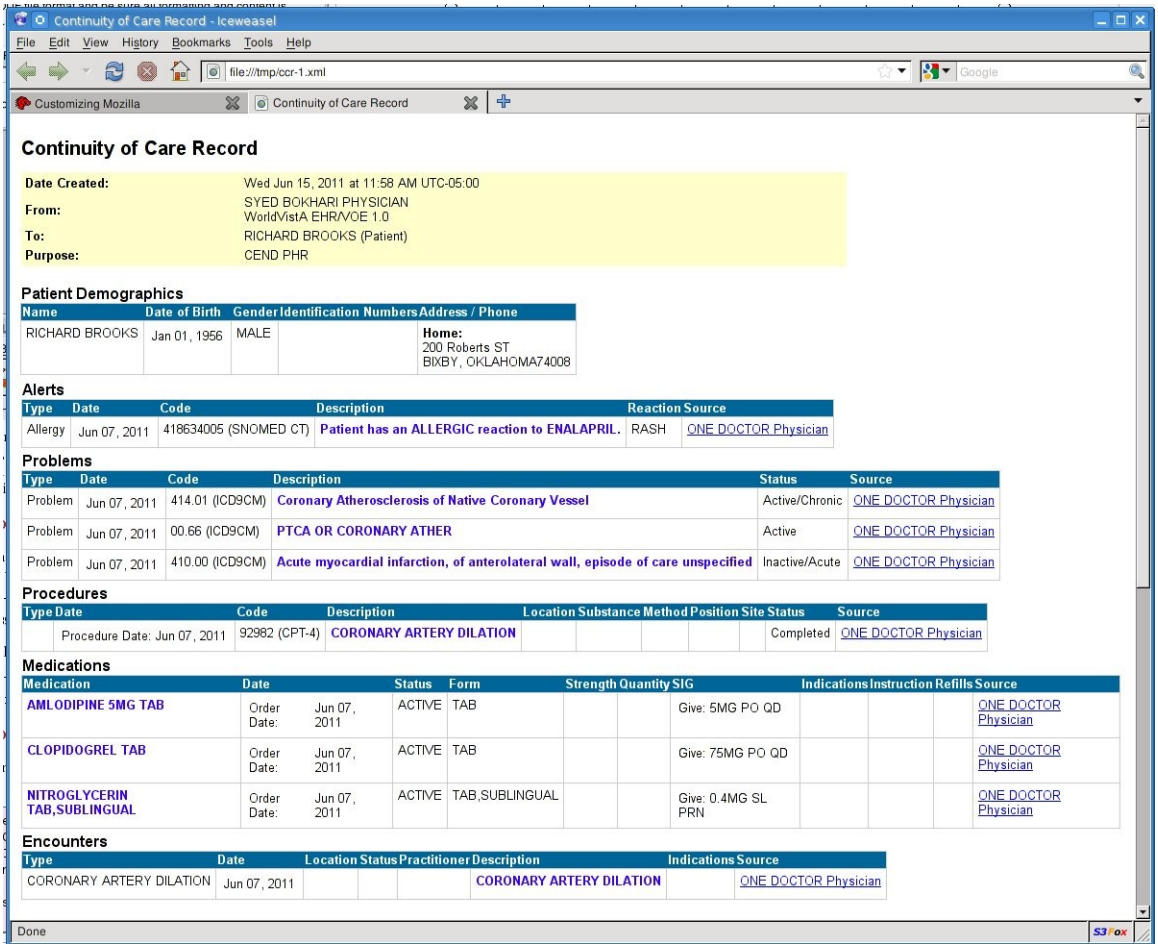
Note on the detailed view that the email is encrypted and signed signified by the padlock and sealed envelope icon.

```
Jun 15 14:41:31 mail2 postfix/tlsmgr[23344]: delete smtpd session id=6AB2C598AA369D6D4AA25B0C08FC433774B2B8F28F7016E0
8090346CF9F11C85&s=smtp
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: initializing the server-side TLS engine
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: connect from gtm[66.206.177.84]
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: setting up TLS connection from gtm[66.206.177.84]
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: gtm[66.206.177.84]: TLS cipher list "ALL:!EXPORT:!LOW:+RC4:@STRENGTH"
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:before/accept initialization
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 read client hello B
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write server hello A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write certificate A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write key exchange A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write server done A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 flush data
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 read client key exchange A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 read finished A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write session ticket A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write change cipher spec A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 write finished A
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: SSL_accept:SSLv3 flush data
Jun 15 14:45:25 mail2 postfix/smtpd[3347]: Anonymous TLS connection established from gtm[66.206.177.84]: TLSv1 with c
ipher DHE-RSA-AES256-SHA (256/256 bits)
Jun 15 14:45:26 mail2 postfix/smtpd[3347]: 399C5101AD: client=gtm[66.206.177.84]
Jun 15 14:45:26 mail2 postfix/cleanup[3350]: 399C5101AD: message-id=<969.3110615@WVEHR309.OPENFORUM.OPENSOURCEVISTA.N
ET>
Jun 15 14:45:26 mail2 postfix/qmgr[23337]: 399C5101AD: from=<BOKHARI.SYED@WVEHR309.OPENFORUM.OPENSOURCEVISTA.NET>, si
ze=13627, nrcpt=1 (queue active)
Jun 15 14:45:26 mail2 postfix/smtp[3351]: 399C5101AD: to=<brooks.richard@SECUREMAIL.OPENSOURCEVISTA.NET>, relay=127.0
.0.1[127.0.0.1]:10025, delay=0.63, delays=0.5/0.02/0.05/0.06, dsn=2.6.0, status=sent (250 2.6.0 Message received)
Jun 15 14:45:26 mail2 postfix/qmgr[23337]: 399C5101AD: removed
Jun 15 14:45:27 mail2 postfix/smtpd[3352]: connect from localhost[127.0.0.1]
Jun 15 14:45:27 mail2 postfix/smtpd[3352]: 60C6A101AD: client=gtm[66.206.177.84]
Jun 15 14:45:27 mail2 postfix/smtpd[3347]: disconnect from gtm[66.206.177.84]
Jun 15 14:45:27 mail2 postfix/cleanup[3350]: 60C6A101AD: message-id=<969.3110615@WVEHR309.OPENFORUM.OPENSOURCEVISTA.N
ET>
Jun 15 14:45:27 mail2 postfix/cleanup[3350]: 60C6A101AD: replace: header Content-Type: application/pkcs7-mime; name="
smime.p7m"; smime-type=enveloped-data from gtm[66.206.177.84]; from=<BOKHARI.SYED@WVEHR309.OPENFORUM.OPENSOURCEVISTA.
NET> to=<brooks.richard@SECUREMAIL.OPENSOURCEVISTA.NET> proto=unknown: Content-Type: application/pkcs7-mime; smime-ty
pe=enveloped-data; name="smime.p7m"
Jun 15 14:45:28 mail2 postfix/qmgr[23337]: 60C6A101AD: from=<BOKHARI.SYED@WVEHR309.OPENFORUM.OPENSOURCEVISTA.NET>, si
ze=27352, nrcpt=1 (queue active)
Jun 15 14:45:28 mail2 postfix/smtpd[3352]: disconnect from localhost[127.0.0.1]
Jun 15 14:45:28 mail2 postfix/local[3353]: 60C6A101AD: to=<brooks.richard@SECUREMAIL.OPENSOURCEVISTA.NET>, relay=loca
l, delay=1.4, delays=1.3/0.03/0/0.08, dsn=2.0.0, status=sent (delivered to mailbox)
Jun 15 14:45:28 mail2 postfix/qmgr[23337]: 60C6A101AD: removed
Jun 15 14:45:54 mail2 dovecot: pop3-login: Login: user=<brooks.richard>, method=PLAIN, rip=96.231.217.75, lip=66.206.
177.87, TLS
Jun 15 14:45:55 mail2 dovecot: POP3(brooks.richard): Disconnected: Logged out top=0/0, retr=2/55096, del=2/2, size=55
060
mail2:/var/log#
```

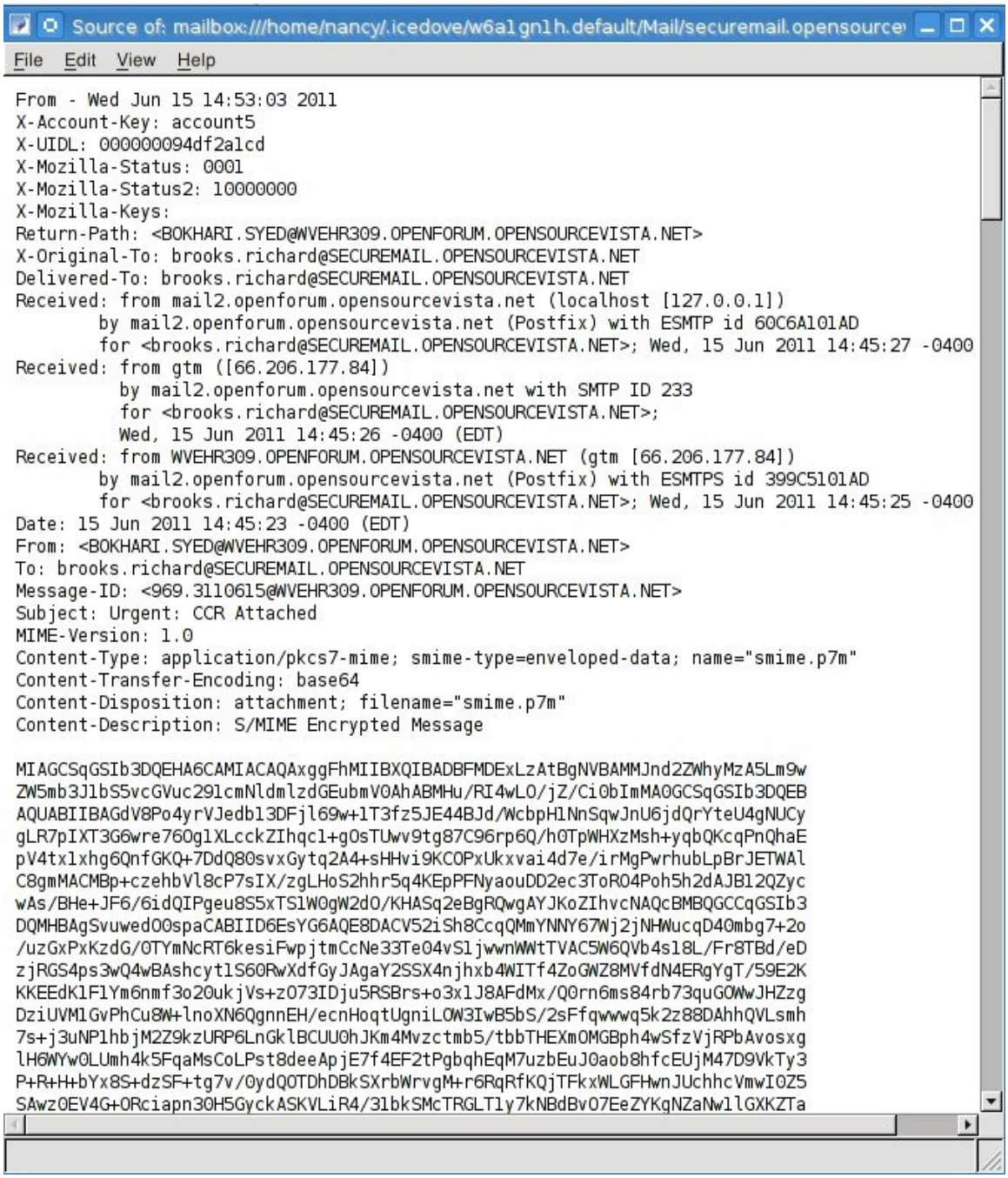
Log Is made of the delivery to the mailbox of the CCR and of the secure pickup of the mail by Richard Brooks.



Double Click on the ccr.xml attachment and click OK.



CCR is displayed for the patient.



Source from the top of the emails showing information about the times and encryption. Etc. This is the same as it was when it was stored on the server in an encrypted format to be sent,