Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων
Εργασία 2

Για την εκπόνηση της εργασίας χρησιμοποιήσαμε λειτουργικό σύστημα Windows.

Στη συνέχεια εγκαταστήσαμε τη Win64OpenSSL_Light-1_0_2a και συνεχίσαμε με τις κατάλληλες ρυθμίσεις αυτής μέσω cmd όπως παρακάτω.
Set OpenSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg.
Καθώς επίσης αλλάξαμε και το αρχείο openssl.cnf γιατί ήταν αναγκαίο.

Παρακάτω,συνεχίσαμε δημιουργώντας τα certificates,τα private και public keys καθώς επίσης και τα requestcertificates όπου χρειαζόντουσαν.

Έτσι λοιπόν αρχίσαμε να φτιάχνουμε τα πρώτα αρχεία τα οποία είναι της Caroot.Παρακάτω βλέπουμε τη δημιουργία του Self-Signed Certificate με τις κατάλληλες παραμέτρους που έπρεπε να ορίσουμε.

```
C:\Users\kots>cd ..

C:\Users>cd ..

C:\>cd OpenSSL-Win64

C:\OpenSSL-Win64>cd bin

C:\OpenSSL-Win64\bin>cd CA0

C:\OpenSSL-Win64\bin\CA0>openssl
```

```
OpenSSL> genrsa -aes256 -out CA0PrivateKey.key 4096
Loading 'screen' into random state - done
Generating RSA private key, 4096 bit long modulus
.....................................................................++
.....................................++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase for CA0PrivateKey.key:
Verifying - Enter pass phrase for CA0PrivateKey.key:
OpenSSL> rsa -in CA0PrivateKey.key -out CA0PublicKey.key
Enter pass phrase for CA0PrivateKey.key:
writing RSA key
OpenSSL> req -new -x509 -nodes -sha1 -key CA0PublicKey.key -out CA0Certificate.c
rt -days 720
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CAroot
Organizational Unit Name (eg, section) []:CAroot
Common Name (e.g. server FQDN or YOUR name) []:CAroot
Email Address []:caroot@yahoo.gr
```

Πάνω πάνω αρχίζουμε με την εντολή genrsa που είναι για την παραγωγή του κλειδιού.Και

στο τέλος της εντολής αυτής του δίνουμε το μέγεθός του.Στη συνέχεια δημιουργούμε το PublicKey απο το PrivateKey που είχαμε δημιουργήσει νωρίτερα.Και τέλος δημιουργούμε το Certificate της CA0 με τις παραμέτρους που χρειάζεται όπως είναι ο αλγόριθμος υπογραφής sha1 αλλά και οι μέρες που θα είναι έγκυρο,στην περίπτωση αυτή 720 δηλαδή 24 μήνες.

Στη συνέχεια,δημιουργήσαμε τα Certificates των άλλων 2 CA(CA1,CA2) οποία έπρεπε να είναι υπογεγγραμένα απο την CA0.

```
OpenSSL> genrsa -out CA1PrivateKey.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
..................+++
....+++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> req -new -key CA1PrivateKey.key -out CA1RequestCertificate.csr
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CA1
Organizational Unit Name (eg, section) []:CA1
Common Name (e.g. server FQDN or YOUR name) []:CA1
Email Address []:ca1@yahoo.gr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:CA1
string is too short, it needs to be at least 4 bytes long
A challenge password []:1234
An optional company name []:CA1
OpenSSL> x509 -req -in CA1RequestCertificate.csr -CA CA0Certificate.crt -CAkey C
A0PublicKey.key -CAcreateserial -out CA1Certificate.crt -days 360
Loading 'screen' into random state - done
Signature ok
subject=/C=gr/ST=gr/L=gr/O=CA1/OU=CA1/CN=CA1/emailAddress=ca1@yahoo.gr
Getting CA Private Key
unable to write 'random state'
```

```
OpenSSL> rsa -in CA1PrivateKey.key -out CA1PublicKey.key
writing RSA key
```

Εδώ βλέπουμε τον τρόπο δημιουργίας της CA1.Πάλι η πρώτη εντολή είναι για να παραχθεί το privatekey το οποίο αυτή τη φορά είναι 2048 bits.Μετά δημιουργούμε πάλι το publickey ,και το αρχείο csr το οποιό είναι αναγκαίο για τη δημιουργία του certificate από τη στιγμή που δεν είναι self signed.Στο τέλος δημιουργήσαμε το certificate του με τις κατάλληλες παραμέτρους πάλι,οι οποίες είναι ο αλγόριθμος sha1 και οι μέρες που θα είναι διαθέσιμο (360 δηλαδή 12 μήνες).Εδώ λοιπόν βλέπουμε πως για να δημιουργηθεί το συγκεκριμένο certificate χρειαζόμαστε το certificate της Caroot αλλά και το PublicKey της συγκεκριμένης.Από κάτω ακολουθεί η οθόνη δημιουργίας και της CA2.

```
OpenSSL> genrsa -out CA2PrivateKey.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....................................+++
.....................................................................................
...........+++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> req -new -key CA2PrivateKey.key -out CA2RequestCertificate.csr
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CA2
Organizational Unit Name (eg, section) []:CA2
Common Name (e.g. server FQDN or YOUR name) []:CA2
Email Address []:ca2@yahoo.gr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:2345
An optional company name []:2345
OpenSSL> x509 -sha1 -req -in CA2RequestCertificate.csr -CA CA0Certificate.crt -C
Akey CA0PublicKey.key -CAcreateserial -out CA1Certificate.crt -days 360
Loading 'screen' into random state - done
Signature ok
subject=/C=gr/ST=gr/L=gr/O=CA2/OU=CA2/CN=CA2/emailAddress=ca2@yahoo.gr
Getting CA Private Key
unable to write 'random state'
OpenSSL> x509 -req -in CA2RequestCertificate.csr -CA CA0Certificate.crt -CAkey C
A0PublicKey.key -CAcreateserial -out CA2Certificate.crt -days 360
Loading 'screen' into random state - done
Signature ok
subject=/C=gr/ST=gr/L=gr/O=CA2/OU=CA2/CN=CA2/emailAddress=ca2@yahoo.gr
Getting CA Private Key
unable to write 'random state'
```

```
OpenSSL> rsa -in CA2PrivateKey.key -out CA2PublicKey.key
writing RSA key
```

Στη συνέχεια δημιουργήσαμε τους 4 χρήστες που για τους 2 πρώτους εκδίδει πιστοποιητικά η CA1 και για τους άλλους 2 η CA2.

User1:

```
OpenSSL> genrsa -out User1PrivateKey.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.++++++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> rsa -in User1PrivateKey.key -out User1PublicKey.key
writing RSA key
OpenSSL> req -new -key User1PrivateKey.key -out User1RequestCertificate.csr
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:USER1
Organizational Unit Name (eg, section) []:USER1
Common Name (e.g. server FQDN or YOUR name) []:USER1
Email Address []:user1@yahoo.gr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:12354
OpenSSL> x509 -req -in User1RequestCertificate.csr -CA CA1Certificate.crt -CAkey
 CA1PublicKey.key -CAcreateserial -out User1Certificate.crt -days 180
Loading 'screen' into random state - done
Signature ok
subject=/C=gr/ST=gr/L=gr/O=USER1/OU=USER1/CN=USER1/emailAddress=user1@yahoo.gr
Getting CA Private Key
unable to write 'random state'
```

User2:

```
OpenSSL> genrsa -out User2PrivateKey.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..............++++++
..............++++++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> rsa -in User2PrivateKey.key -out User2PublicKey.key
writing RSA key
OpenSSL> req -new -key User2PrivateKey.key -out User2RequestCertificate.csr
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:USER2
OpenSSL> genrsa -out User3PrivateKey.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.......++++++
....++++++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> rsa -in User3PrivateKey.key -out User3PublicKey.key
writing RSA key
OpenSSL> req -new -key User3PrivateKey.key -out User3RequestCertificate.csr
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:User3
Organizational Unit Name (eg, section) []:User3
Common Name (e.g. server FQDN or YOUR name) []:User3
Email Address []:user3@yahoo.gr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:1234
OpenSSL> x509 -req -in User3RequestCertificate.csr -CA CA2Certificate.crt -CAkey
 CA2PublicKey.key -CAcreateserial -out User3Certificate.crt -days 180
Loading 'screen' into random state - done
Signature ok
subject=/C=gr/ST=gr/L=gr/O=User3/OU=User3/CN=User3/emailAddress=user3@yahoo.gr
Getting CA Private Key
unable to write 'random state'
```

User3:

User4:

```
OpenSSL> genrsa -out User4PrivateKey.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
........++++++
......++++++
unable to write 'random state'
e is 65537 (0x10001)
OpenSSL> rsa -in User4PrivateKey.key -out User4PublicKey.key
writing RSA key
OpenSSL> req -new -key User4PrivateKey.key -out User4RequestCertificate.csr
Loading 'screen' into random state - done
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) [AU]:gr
State or Province Name (full name) [Some-State]:gr
Locality Name (eg, city) []:gr
Organization Name (eg, company) [Internet Widgits Pty Ltd]:User4
Organizational Unit Name (eg, section) []:User4
Common Name (e.g. server FQDN or YOUR name) []:User4
Email Address []:user4@yahoo.gr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:1234
OpenSSL> x509 -req -in User4RequestCertificate.csr -CA CA2Certificate.crt -CAkey
 CA2PublicKey.key -CAcreateserial -out User4Certificate.crt -days 180
Loading 'screen' into random state - done
Signature ok
subject=/C=gr/ST=gr/L=gr/O=User4/OU=User4/CN=User4/emailAddress=user4@yahoo.gr
Getting CA Private Key
unable to write 'random state'
```

Ο τρόπος δημιουργίας τους είναι ο ίδιος με της CA1 και της CA2 αλλάζοντας απλά τις κατάλληλες παραμέτρους.Παρακάτω βλέπουμε τον τρόπο μετακίνησης κάθε αρχείου στον κατάλληλο φάκελο.

```
C:\OpenSSL-Win64\bin\CA0>mkdir User1
```

```
C:\OpenSSL-Win64\bin\CA0>move User1PrivateKey.key User1
        1 file(s) moved.

C:\OpenSSL-Win64\bin\CA0>move User1PublicKey.key User1
        1 file(s) moved.

C:\OpenSSL-Win64\bin\CA0>move User1Certificate.crt User1
        1 file(s) moved.

C:\OpenSSL-Win64\bin\CA0>move User1RequestCertificate.csr User1
        1 file(s) moved.
```

Το ίδιο έγινε για όλα τα αρχεία.

Ερώτημα 3

Σε αυτό το ερώτημα μας ζητήθηκε η επαλήθευση της αυθεντικότητας του χρήστη 3 από τον χρήστη 1 ενώ ανήκουν σε διαφορετικές αρχές πιστοποίησης.
Ο τρόπος για το συγκεκριμένο ερώτημα είναι ο παρακάτω:

1. Επαλήθευση του χρήστη 1 από την CA1
2. Επαλήθευση της CA1 από την CA0
3. Επαλήθευση της CA0 από την CA2
4. Επαλήθευση της CA2 από τον χρήστη 3

Όπως φαίνεται και παρακάτω.

```
OpenSSL> verify -CAfile CA1/CA1PrivateKey.key User1/User1PrivateKey.key
OpenSSL> verify -CAfile CA0/CA0PrivateKey.key CA1/CA1PrivateKey.key
OpenSSL> verify -CAfile CA2/CA2PrivateKey.key CA0/CA0PrivateKey.key
OpenSSL> verify -CAfile User3/User3PrivateKey.key CA2/CA2PrivateKey.key
```

Ερώτημα 4

Σε αυτό το ερώτημα μας ζητήθηκε η δημιουργία μιας λίστας CRL για την ανάκληση πιστοποιητικού του χρήστη 4.Όπως φαίνεται παρακάτω.

```
OpenSSL> ca -keyfile CA2/CA2PrivateKey.key -cert CA2/CA2Certificate.crt -gencrl
-out mycrl.pem
Using configuration from C:\OpenSSL-Win64\bin\openssl.cfg
Loading 'screen' into random state - done
```

Εδώ γίνεται η δημιουργία της crl από την αρχή πιστοποίησης CA2.

```
OpenSSL> ca -revoke User4/User4Certificate.crt -keyfile CA2/CA2PublicKey.key -ce
rt CA2/CA2Certificate.crt
Using configuration from C:\OpenSSL-Win64\bin\openssl.cfg
Loading 'screen' into random state - done
```

Και εδώ κάνουμε revoke το certificate του User4.

Ερώτημα 5

Σε αυτό το ερώτημα μας ζητήθηκε όπως και στο ερώτημα 3 η επαλήθευση του χρήστη 4 από τον χρήστη 2.Ο τρόπος είναι ακριβώς ο ίδιος όπως και στο ερώτημα 3 απλά με τη διαφορά πως αφού έχει προηγηθεί η ανάκληση πιστοποιητικού του χρήστη 4,η επαλήθευση αυτή δεν γίνεται επιτυχώς.