Setting up signed and encrypted email with openssl, part 1. by Philippe Bogaerts, alias xxradar. http://www.radarhack.com mailto:xxradar@radarhack.com. Version 1.0 20-09-2003

1. Introduction

Spending months in studying PKI and certificate related stuff, I started using openssl to do it 'by hand' instead of with a fancy GUI. I came across so many interesting articles and other things that did not work, that I decided to write down what actually worked. This is an introduction paper, explaining the install and basic configuration of an openssl based CA and generating certificates for use in Outlook.

2. Installing openssl

You can obtain openssl for win32 by doing a search on google. There is a simple release, a zip file containing the binary and some DLL's. I also found a version with a setup program. If you install it manually, make sure that the DLL files are copied into the %system%\system32 directory. Also take a look at <u>http://www.openssl.org</u> of course.

- Install openssl in a directory, for example c:\openssl
- Create a subdirectory, for example my_ca c:\openssl\my_ca
- Create within c:\openssl\my_ca\ the following subdirectories
 certs
 crl
 csr
 newcerts
 private

- Create in c:\openssl\my_ca\ a file "index.txt" with nothing in (0 bytes length). Type "notepad index.txt", create the file and save. Verify that the file totally empty. You can also try "copy con index.txt" followed by ctrl+z.

- Create in c:\openssl\my_ca\ a file "serial" starting with 01. Type echo 01 >serial

- Then create or edit the c:\openssl\openssl.cnf and edit the file, to reflect the directory layout as above stated. Be careful, there are so many examples on the internet that do not seem to work on win32.

Here is a sample openssl.cnf file (tested on W2k sp4)

#
SSLeay example configuration file.
This is mostly being used for generation of certificate requests.
#

RANDFILE = .rnd

dir	=	./my_ca	#	Where everything is kept
certs	=	\$dir/certs	#	Where the issued certs are kept
crl_dir	=	\$dir/crl	#	Where the issued crl are kept
database	=	\$dir/index.txt	#	database index file.
new_certs_dir	=	\$dir/newcerts	#	default place for new certs.

certificate = \$dir/certs/ca.crt # The CA certificate serial = \$dir/serial # The current serial number crl = \$dir/crl.pem # The current CRL private_key = \$dir/private/cakey.key # The private key RANDFILE = \$dir/private/private.rnd # private random number file x509_extensions = x509v3_extensions # The extentions to add to the cert default_days = 365 # how long to certify for default_crl_days = 30 # how long before next CRL default_md = md5 # which md to use. preserve = no # keep passed DN ordering # A few difference way of specifying how similar the request should look # For type CA, the listed attributes must be the same, and the optional # and supplied fields are just that :-) policy = policy_match *#* For the CA policy [policy_match] countryName = optional stateOrProvinceName = optional
organizationName = optional organizationalUnitName = optional commonName = supplied
emailAddress = optional # For the 'anything' policy # At this point in time, you must list all acceptable 'object' # types. [policy_anything] = optional countryName stateOrProvinceName = optional localityName = optional localityName = optional
organizationName = optional organizationalUnitName = optional = supplied commonName emailAddress = optional ****** [reg] default bits = 1024default_keyfile = privkey.pem distinguished_name = req_distinguished_name = req_attributes attributes [req_distinguished_name] countryName = Country Name (2 letter code) countryName_min= 2countryName_max= 2stateOrProvinceName= State or Province Name (full name)localityName= Locality Name (eg, city)organizationName= Organization Name (eg, company) organizationalUnitName = Organizational Unit Name (eg, section) commonName = Common Name (eg, your website's domain name) commonName_max = 64 emailAddress = Email Address emailAddress_max = 40

[req_attributes]
challengePassword = A challenge password
challengePassword_min = 4
challengePassword_max = 20

[x509v3_extensions]

under ASN.1, the 0 bit would be encoded as 80
#nsCertType
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName
#nsCertSequence
#nsCertExt
#nsDataType

The installation process is done. We are ready to start building our CA.

3. Create a CA certificate and keys. Once this done, we must create our CA keys and a CA root certificate. First of all, generate RSA keys for the CA. C:\openssl>openssl genrsa -des3 -out ./my_ca/private/cakey.key 2048 Loading 'screen' into random state - done warning, not much extra random data, consider using the -rand option Generating RSA private key, 2048 bit long modulus ...+++ e is 65537 (0x10001) Enter PEM pass phrase: Verifying password - Enter PEM pass phrase: C:\openssl> Once we have a key pair, we can generate the CA certificate. C:\openssl>openssl req -new -x509 -days 365 -key ./my_ca/private/cakey.key -out ./my_ca/certs/ca.crt Using configuration from ./openssl.cnf 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) [AU]:be State or Province Name (full name) [Some-State]:br Locality Name (eg, city) []:my_town Organization Name (eg, company) [Internet Widgits Pty Ltd]:radarhack.com Organizational Unit Name (eg, section) []:r&d Common Name (eg, YOUR name) []:my_ca Email Address []: C:\openssl> Make sure this .crt file as well as the key is reflected in the openssl.cnf file. [CA_default] dir # Where everything is kept = ./my_ca = \$dir/certs *# Where the issued certs are kept* certs = \$dir/certs # where the issued certs are kept crl_dir = \$dir/index.txt # database index file. database new_certs_dir = \$dir/newcerts # default place for new certs. certificate = \$dir/certs/ca.crt # The CA certificate # The current serial number serial = \$dir/serial = \$dir/crl.pem # The current CRL crl = **\$dir/private/cakey.key** # The private key private_key RANDFILE = \$dir/private/private.rnd *# private random number* . .

This is the CA's root certificate. This certificate must be distributed to everyone that should trust this CA in a secure manner. Copy (or distribute via http (not secure) the file to the client computers and install the certificate by double clicking or C:\openssl\my_ca\certs>start ca.crt

Certificate	? ×
General Details Certification Path	
Certificate Information	
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
Issued to: my_ca	-
Issued by: my_ca	
Valid from 9/11/2003 to 9/10/2004	
Install Certificate Issuer State	ment
	ок

After clicking Install Certificate (and trusting the CA certificate) it will show up in IE.

Go to Tools->Content->Certificates->Trusted Root Certification Authorities

Issued To	Issued By	Expiratio	Friendly Name	
IPS SERVIDORES KMD-CA Kvalificeret KMD-CA Root KMD-CA Server Microsoft Authentic Microsoft Root Auth Microsoft Root Certi Microsoft Root Certi Microsoft Root Certi Microsoft Root Certi NetLock Express2 (IPS SERVIDORES KMD-CA Kvalificeret P KMD-CA Root KMD-CA Server Microsoft Authenticod Microsoft Root Authority Microsoft Root Certifi my_ca NetLock Express2 (Cla	12/30/2009 11/23/2015 7/11/2022 10/12/2018 1/1/2000 12/31/2020 5/10/2021 9/10/2004 2/20/2019	IPS SERVIDORES KMD-CA K Person KMD-CA Root KMD-CA Server Microsoft Authe Microsoft Root A Microsoft Root C <none> NetLock Express</none>	
Import Export	<u>R</u> emove		Advan	ced

4. Create certificates for the users.

Generate a key for a user or server. There is no technical difference in server certificates compared to user certificates. The CN will contain the F.Q.D.N. for servers, and the user name for users.

Generate a CSR for user1 (certificate signing request)

C:\openssl>openssl req -new -key .\my_ca\private\user1.key -out .\my_ca\csr\user1.csr Using configuration from .\openssl.cnf Enter PEM pass phrase: (to unlock user1.key) 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]:be State or Province Name (full name) [Some-State]:br Locality Name (eg, city) []:my_town Organization Name (eg, company) [Internet Widgits Pty Ltd]:radarhack.com Organizational Unit Name (eg, section) []:r&d Common Name (eg, YOUR name) []:xxradar Email Address []:xxradar@radarhack.com

Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []:

C:\openssl>

The next step is to sign the certificate

C:\openssl>openssl ca -config .\openssl.cnf -policy policy_anything -out .\my_ca\newcerts\user1.pem -infiles .\my_ca\csr\user1.csr Using configuration from .\openssl.cnf Loading 'screen' into random state - done Enter PEM pass phrase: (to unlock cakey.key) Check that the request matches the signature Signature ok The Subjects Distinguished Name is as follows countryName :PRINTABLE: 'be' stateOrProvinceName :PRINTABLE: 'br' :T61STRING: 'my_town' localityName :PRINTABLE: 'radarhack.com' organizationName organizationalUnitName:T61STRING:'r&d' :PRINTABLE: 'xxradar' commonName emailAddress :IA5STRING: 'xxradar@radarhack.com' (must match an email account in outlook) Certificate is to be certified until Sep 15 18:34:59 2004 GMT (365 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y Write out database with 1 new entries Data Base Updated

Converting certificates from PEM to DER or PKCS#12, to make them Microsoft ready.

C:\openssl>openssl pkcs12 -export -in ./my_ca/newcerts/user1.pem -inkey ./my_ca/private/user1.key -out ./my_ca/newcerts/user1.p12 Loading 'screen' into random state - done Enter PEM pass phrase: (to unlock user1.key) Enter Export Password: (to protect PKCS#12 file) Verifying password - Enter Export Password:

Do the same thing for a user2.

Installing the certificates in your email client. Once you have an email account for a user, install the certificate in the personal certificate store, by double clicking the PKCS#12 file.

And the second	
Specify the file you want to impo	ərt.
File name:	
C:\openssl\my_ca\newcerts\us	er1.p12 Browse
Note: More than one certificate	can be stored in a single file in the following format
Personal Information Exchange	ge- PKCS #12 (.PFX, .P12)
Cryptographic Message Synta	ax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificat	e Store (.SST)
	<back next=""> Ca</back>
ate Import Wizard	
cate Import Wizard tificate Store	
cate Import Wizard rtificate Store Cartificate stores are system are	eas where certificates are kept.
cate Import Wizard rtificate Store Certificate stores are system are Windows can automatically selec	eas where certificates are kept .
cate Import Wizard tificate Store Certificate stores are system an Windows can automatically selec C. Automatically select the c	eas where certificates are kept.
Cate Import Wizard tificate Store Certificate stores are system are Windows can automatically selec C Automatically select the c Place all certificates in the	eas where certificates are kept. It a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store
Cate Import Wizard tificate Store Certificate stores are system and Windows can automatically select Automatically select the o Place all certificates in the Certificate store:	eas where certificates are kept. ct a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store
Cate Import Wizard rtificate Store Certificate stores are system an Windows can automatically select C Automatically select the c Place all certificates in the Certificate store: Personal	eas where certificates are kept. It a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store Browse
Cate Import Wizard rtificate Store Certificate stores are system and Windows can automatically select Automatically select the of Place all certificates in the Certificate store: Personal	eas where certificates are kept. It a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store Browse
Cate Import Wizard rtificate Store Certificate stores are system are Windows can automatically select Automatically select the c Place all certificates in the Certificate store: Personal	eas where certificates are kept. It a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store Browse
Cate Import Wizard rtificate Store Certificate stores are system an Windows can automatically select Automatically select the c Place all certificates in the Certificate store: Personal	eas where certificates are kept. It a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store Browse
Cate Import Wizard rtificate Store Certificate stores are system and Windows can automatically select Automatically select the of Place all certificates in the Certificate store: Personal	eas where certificates are kept. It a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store Browse
Cate Import Wizard rtificate Store Certificate stores are system are Windows can automatically select Automatically select the c Place all certificates in the Certificate store: Personal	eas where certificates are kept. ct a certificate store, or you can specify a location fo certificate store based on the type of certificate a following store Browse

Verify the certificate by checking IE.

ssued To	Issued By	Expiratio	Friendly Name
Administrator	Administrator	6/11/2103	<none></none>
pbogaertike	ip3309nyv4r	7/7/2004	AKS ifdh 1::pbog
pbogaerts_notebook	ip3309nyv4r	2/16/2005	pbogaerts_note
		7/9/2004	AKS ifdh 1::Tha
Thawte Freemail Me	Personal Freemail RS	1112001	
Thawte Freemail Me Thawte Freemail Me	Personal Freemail RS Personal Freemail RS	7/9/2003	AKS ifdh 1::Tha
 Thawte Freemail Me Thawte Freemail Me xxradar 	Personal Freemail RS Personal Freemail RS my_ca	7/9/2003 9/15/2004	AKS ifdh 187ha <none></none>

Double click the certificate and take a look.



You can check the certification path as shown.

ertificate	? >
General Details Certification Path	
Certification path	_
🖼 my_ca	
View Certif	icate
Certificate status	
This certificate is OK.	
	ОК

Last but not least, use the certificate for encryption/signing on the mail account.

General Servers	Connection Secu	nity Advance	d]
Signing certificat	•		
Select the sig ID used when	ning certificate below. signing messages wit	This will detern h this account.	nine the digital
Certificate:	sxradar		Select
Encrypting prefe	rences		
Select the end included with encrypted mail	styption certificate and your digitally signed mi I to you with these set	l algorithm. The essages so oth tings.	ise are ers can send
	-		
Certificate:	12		Select
Certificate: Algorithm:	3DES	<u> </u>	Select
Certificate: Algorithm:	3DES		Select
Certificate: Algorithm:	JDES		Select

Remember to-do the same thing for a second user. You can create a second email account in the same outlook client, if you have two email accounts available. HAVE FUN!