Curs 10
Demo PKI & TLS

Gestiunea serviciilor de rețea (GSR)
15 decembrie 2016

Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

Crearea unui Root CA

Demo

Crearea unui Intermediate CA

Demo

Crearea unui certificat digital

Demo

Cuprins

Configurarea unui server web pentru TLS

Demo

Configurarea unui MTA pentru TLS

Demo

Cuprins

Exemplu - /home/certs/ca/root/openssl.conf

```
[ ca ]
default_ca = CA_default

[ CA_default ]
dir               = /home/certs/ca/root
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand
private_key       = $dir/private/ca.key.pem
certificate       = $dir/certs/ca.cert.pem
crlnumber         = $dir/crlnumber
crl               = $dir/crl/ca.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30
default_md        = sha256
name_opt          = ca_default
cert_opt          = ca_default
default_days      = 375
preserve          = no
policy            = policy_strict

[ policy_strict ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ policy_loose ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits        = 2048
distinguished_name  = req_distinguished_name
string_mask         = utf8only
default_md          = sha256
x509_extensions     = v3_ca

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
stateOrProvinceName             = State or Province Name
```

```
localityName                    = Locality Name
0.organizationName              = Organization Name
organizationalUnitName          = Organizational Unit Name
commonName                      = Common Name
countryName_default             = RO
stateOrProvinceName_default     = Bucharest
localityName_default            = Bucharest
0.organizationName_default      = GSR CA
organizationalUnitName_default  = Gestiunea Serviciilor de Retea

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ usr_cert ]
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

[ server_cert ]
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

[ crl_ext ]
authorityKeyIdentifier=keyid:always

[ ocsp ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

Exemplu - /home/certs/ca/intermediate/openssl.conf

```
[ ca ]
default_ca = CA_default

[ CA_default ]
dir               = /home/certs/ca/intermediate
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand
private_key       = $dir/private/intermediate.key.pem
certificate       = $dir/certs/intermediate.cert.pem
crlnumber         = $dir/crlnumber
crl               = $dir/crl/intermediate.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30
default_md        = sha256
name_opt          = ca_default
cert_opt          = ca_default
default_days      = 375
preserve          = no
policy            = policy_loose

[ policy_strict ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ policy_loose ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits        = 2048
distinguished_name  = req_distinguished_name
string_mask         = utf8only
default_md          = sha256
x509_extensions     = v3_ca

[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
stateOrProvinceName             = State or Province Name
localityName                    = Locality Name
0.organizationName              = Organization Name
organizationalUnitName          = Organizational Unit Name
commonName                      = Common Name
countryName_default             = RO
stateOrProvinceName_default     = Bucharest
localityName_default            = Bucharest
0.organizationName_default      = GSR Intermediate CA
organizationalUnitName_default  = GSR CA Service

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ usr_cert ]
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

[ server_cert ]
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

[ crl_ext ]
authorityKeyIdentifier=keyid:always

[ ocsp ]
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

Exemplu - comenzi pentru generarea certificatelor (1)

Root CA

```
~/ca/root$ openssl genrsa -aes256 -out private/ca.key.pem 4096

~/ca/root$ openssl req -config openssl.conf -key private/ca.key.pem
-new -x509 -days 7300 -sha256 -extensions v3_ca -out certs/ca.cert.pem

~/ca/root$ openssl x509 -noout -text -in certs/ca.cert.pem
```

Exemplu - comenzi pentru generarea certificatelor (2)

Intermediate CA (1)

```
~/ca/intermediate$ openssl genrsa -aes256
-out private/intermediate.key.pem 4096

~/ca/intermediate$ openssl req -config openssl.conf -new -sha256
-key private/intermediate.key.pem -out csr/intermediate.csr.pem

~/ca/intermediate$ openssl ca -config ../root/openssl.conf
-extensions v3_intermediate_ca -days 3650 -notext -md sha256
-in csr/intermediate.csr.pem -out certs/intermediate.cert.pem

~/ca/intermediate$ openssl genrsa -aes256
-out private/mail.root.gsr.key.pem 2048
```

Exemplu - comenzi pentru generarea certificatelor (3)

Intermediate CA (2)

```
~/ca/intermediate$ openssl req -config openssl.conf
-key private/mail.root.gsr.key.pem -new -sha256
-out csr/mail.root.gsr.csr.pem

~/ca/intermediate$ openssl ca -config openssl.conf
-extensions server_cert -days 375 -notext -md sha256
-in csr/mail.root.gsr.csr.pem -out certs/mail.root.gsr.cert.pem

~/ca/intermediate$ openssl x509 -noout -text -in certs/mail.root.gsr.cert.pem
```

Resurse utile

- TODO