Wdrożenie architektury EuroPKI-LDAP na podstawie wdrożenia We Wrocławskim Centrum Sieciowo-Superkomputerowym

Autor: Tomasz Kowal
Email: Tomasz.Kowal@pwr.wroc.pl

Wersja 0.1

Wstęp

W ramach projektów NASTEC i „Wdrożenie protokołu LDAP w akademicko-naukowych sieciach komputerowych w Polsce" we Wrocławskim Centrum Sieciowo-Superkomputerowym wdrożona została architektura EuroPKI-LDAP.

Elementy architektury EuroPKI-LDAP

W skład architektury wchodzą obecnie:

- Polskie Centrum Certyfikacji EuroPKI, składające się z serwer CA Front End oraz CA Back End (CA Manager)
  - Centrum Rejestracyjne
    - Aplikacja RA client
    - Serwer RA-SSLFTP
  - Serwer ldap europki (ldap.europki.pl)
- Serwer usługi katalogowej dla Politechniki Wrocławskiej, powstały w ramach wdrożenia.

Procedura wydawania certyfikatu CA dla centrów certyfikacji

Aby uzyskać status Urzędu Certyfikacji EuroPKI upewnij się, że jest przyjęte postępownie wg Polityki Certyfikacji Polskiego Centrum Certyfikacji EuroPKI. W załączniku *Załącznik 1* znajduję się Polityka Polskiego Centrum Certyfikacji EuroPKI. Urząd ubiegający się o certyfikat może posiadać politykę certyfikacji i wydawać certyfikaty różne od Polskiego Centrum Certyfikacji EuroPKI, ale bezpieczniejsze i bardziej restrykcyjne niż certyfikaty Polskiego Centrum Certyfikacji EuroPKI. Urząd ubiegający się musi okresowo przesyłać do Polskiego Centrum Certyfikacji EuroPKI własną politykę w celu weryfikacji, że określona polityka jest stosowana w praktyce.

Procedura podpisania Certyfikatu urzędu certyfikacji:
Urząd ubiegający się o przyłączenie do EuroPKI powinien:

1. wygenerować swoją parę kluczy (akceptowane są TYLKO klucze o długości 2048 bitów);
2. wygenerować wniosek o certyfikat w formacie PKCS#10;
3. uważnie przeczytać i wypełnić deklarację (w *Załączniku 2*);
4. wykonać kopię dokumentu tożsamości ze zdjęciem osoby składającej deklarację (*w Załączniku 3*);
5. uważnie przeczytać i wypełnić wniosek o certyfikat;
6. wykonać kopię dokumentu tożsamości ze zdjęciem osoby składającej wniosek;
7. przesłać e-mailem plik wygenerowany w kroku 2. na adres: europki@pwr.wroc.pl;
8. przesłać pocztą przygotowane w krokach 3-6 dokumenty na adres:
   Polskie Centrum Certyfikacji EuroPKI
   Wrocławskie Centrum Sieciowo-Superkomputerowe
   Politechnika Wrocławska
   Wybrzeże Wyspiańskiego 27
   50-370 Wrocław
   oraz faxem na numer: +48 71 322 57 97

Procedura instalacji oprogramowania do prowadzenie CA, CA Front End i CA Back End

Oprogramowanie zostało uzyskane w ramach projektu NASTEC.

- **Wymagane oprogramowanie na CA Front End - CAFE i CA Back End - CABE**

CABE:

perl, mtools, gzip, tar, vim, standardowy apache, openssl 0.9.6b – **UWAGA!!!** Jest to wersja starsza niż obecna np. w debianie woody, wersja 0.9.6g z debian ma błąd parsera ASN

CAFE:

perl, mtools, gzip, tar, vim, wget, openssl (może być 0.9.6g), apache z wkompilowanym mod_ssl-em (a nie mod_ssl ładowanym z modułu) oraz z obsługa biblioteki pamięci dzielonej mm.

```
# cd sources/mm-wersja/
# ./configure --prefix=/usr/local \
            --disable-shared
# make
# make test
# make install
# cd ../openssl-wersja/
# ./config
# make
# make test
# make install
# cd ../mod-ssl-wersja/
# ./configure --with-apache=../apache-wersja \
            --with-ssl=../openssl-wersja \
            --with-mm=../mm-wersja \
            --prefix=/usr/local/apache
# cd ../apache-wersja
# make
# make certificate
# make install
```

Prawidlowo skompilowany apache powinien miec:

```
/usr/local/mount/apache/bin/httpd –l:
Compiled-in modules:
http_core.c
mod_env.c
mod_log_config.c
mod_mime.c
mod_negotiation.c
mod_status.c
mod_include.c
mod_autoindex.c
mod_dir.c
mod_cgi.c
```

mod_asis.c
mod_imap.c
mod_actions.c
mod_userdir.c
mod_alias.c
mod_access.c
mod_auth.c
mod_setenvif.c
mod_ssl.c

- **Katalog certyfikatu CA EuroPKI na maszynie CABE**

mkdir /root/certyfikaty/
mkdir /root/certyfikaty/CA_EuroPKI

- **Edycja pliku konfiguracyjnego openssl.cnf dla zlecenia certyfikacji CA EuroPKI**

cp /etc/ssl/openssl.cnf /root/certyfikaty/CA _EuroPKI
vim /root/certyfikaty/CA_EuroPKI/openssl.cnf
[req]
default_bits = 2048
[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = PL
countryName_min = 2
countryName_max = 2
0.organizationName = Organization Name (eg, compan y)
0.organizationName_default = CA
commonName = Common Name (eg, YOUR name)
commonName_max = 64
commonName_default = CA EuroPKI
[req_attributes]
#challengePassword = A challenge passwor d
#challengePassword_min = 4
#challengePassword_max = 20

- **Generacja klucza prywatnego CA EuroPKI i zlecenia certyfikacji CA EuroPKI**

cd /root/certyfikaty/<CA>_EuroPKI/
openssl req -nodes -config openssl.cnf -new -keyout klucz.pem -out zlecenie.pem

- **Wysłanie zlecenia certyfikacji do Polskiego Centrum Certyfikacji EuroPKI**

Wyślij e-mailem plik zlecenie.pem na adres: europki@pwr.wroc.pl

- **Pobranie certyfikatu CA EuroPKI ze strony Polskiego Centrum Certyfikacji EuroPKI**

CAFE:

mkdir /root/certyfikaty/
mkdir /root/certyfikaty/CA_EuroPKI
Pobierz certyfikat centrum certyfikacji CA EuroPKI http://www.europki.pl/polish_ca/certs/ca/pl_index.html do pliku ca_cert.pem
ls /root/certyfikaty/CA_EuroPKI
ca_cert.pem

- **Konwersja certyfikatu EuroPKI na pozostałe formaty i stworzenie łańcucha certyfikatów – p7b**

cd /root/certyfikaty/CA_EuroPKI
openssl x509 -text -in ca_cert.pem -out ca_cert.txt
openssl x509 -outform DER -in ca_cert.pem -out ca_cert.der

wget http://www.europki.pl/polish_ca/ca_cert/ca_cert.pem -O Polish_ca_cert.pem

wget http://www.europki.org/ca/root/ca_cert/ca_cert.pem -O Root_ca_cert.pem

openssl crl2pkcs7 -outform DER -nocrl -certfile ca_cert.pem –certfile Polish_ca_cert.pem -certfile Root_ca_cert.pem -out ca_chain.cer

cp ca_chain.cer ca_chain.p7b

–**Stworzenie łańcucha certyfikatów – konkatenacji (potrzebne dla serwera apache)**

cd /root/certyfikaty/CA_EuroPKI

cat ca_cert.pem > chain.crt

cat Polish_ca_cert.pem >> chain.crt

cat Root_ca_cert.pem >> chain.crt

–**Stworzenie użytkowników i grup httpd i httpsd na CAFE**

adduser httpd

adduser httpsd

–**Stworzenie użytkownika i grupy ca_ca na CABE**

adduser ca_ca

–**Katalog źródłowy CAFE**

cd /usr/local/mount/cafe_src/cafe-2.1.3a-ldap-test_softu

–**Edycja pliku konfiguracyjnego CAFE**

cd /usr/local/mount/cafe_src/cafe-2.1.3a-ldap-test_softu

vim config

UWAGA!!!

W CA_DN, należy wpisać DN, takie jak znajdujące się w certyfikacie CA.

Plik config jest plikiem wejściowym dla sed-a.

s/%CA_DN%/CN=CA EuroPKI, O=CA, C=PL/g

s/%CA_RA_DN%//g

s/%CA_OPER_DN%//g

s/%CA_SERVER_NAME%/ca.europki.pl/g

s/%CA_SERVER_URL%/http:\/\/ca.europki.pl/g

s/%CA_SERVER_URL_SEC%/https:\/\/c.europki.pl/g

s/%CA_URL%/http:\/\/ca.europki.pl/g

s/%CA_IMG%/logo.gif/g

s/%CA_SERVER_ADM_MAIL%/europki@ca.pl/g

s/%CA_DIR%/ca_ca/g

s/%CA_NAME%/ca_ca/g

s/%RA_NAME%/ca_ra/g

s/%RA_USERGID%/ca_rausers/g

s/%CA_SUP_MAIL%/europki@ca.pl/g

s/%CA_SUP_FON%/+48 *****/g

s/%CA_SUP_FAX%/+48 *****/g

s/%CA_HOST_URL%/http:\/\/www.ca.pl/g

s/%CA_HOST_ORG_URL%/http:\/\/www.ca.pl/g

s/%CA_HOST_MAIL%/europki@ca.pl/g

s/%CA_HOST_NAME%/CA/g

s/%CA_HOST_ORG%/CA/g

s/%CA_RESPON_NAME%/CA EuroPKI/g

s/%CA_DEPARTMENT%/CA/g

s/%CA_RESPON_PLACE%/CA/g

s/%CA_RESPON_STREET%/*****/g

s/%CA_RESPON_CAPSITY%/******/g
s/%CA_RESPON_PHONE%/+48******/g
s/%CA_RESPON_FAX%/+48 ******/g
s/%INSTALL_DIR%/usr\/local\/mount/g
s/%USER%/httpd/g
s/%USER_SEC%/httpsd/g
s/%PERL_BIN%/\/usr\/bin\/perl/g
s/%SHELL_PATH%/\/bin\/sh/g
s/%APACHE_PATH%/\/usr\/local\/mount\/apache/g
s/%SECUDE_PATH%//g
s/%OPENSSL_PATH%/\/usr\/bin/g
s/%RA_HOME_PATH%/\/usr\/local\/mount\/ra/g
s/%MV_PATH%/\/bin\/mv/g
s/%CHOWN_PATH%/\/bin\/chown/g
s/%CAT_PATH%/\/bin\/cat/g
s/%LDAP_PATH%/\/usr\/sbin/g
s/%LDAP_SERVER%/ldap.ca.europki.pl/g
s/%LDAP_PORT%/389/g
s/%LDAP_BASE%/c=PL/g
s/%LDAP_ROOT_DN%/Manager,c=PL/g
s/%LDAP_ROOT_PASSWORD%/qwerty/g
s/%LDAP_COUNTRY_DN%/PL/g
s/%LDAP_ORG_DN%/o=CA,c=PL/g
s/%TMP_DIR%/\/usr\/local\/tmp/g
s/%EN_CA_NAME%/CA EuroPKI/g
s/%PL_CA_NAME%/CA EuroPKI/g
s/%PL_CA_HOST_ORG%/CA/g
s/%PL_CA_HOST_NAME%/CA/g
s/%PL_CA_RESPON_NAME%/CA EuroPKI/g
s/%PL_CA_DEPARTMENT%/CA/g
s/%PL_CA_RESPON_PLACE%/CA/g
s/%CA_RESPON_COUNTRY%/POLAND/g

- **Tłumaczenie CAFE**

Stworzyć pliki: pl_cp.doc, pl_cps.doc i skopiować
cp pl_cp.doc pl_cps.doc /usr/local/mount/cafe/data/ ca_ca/cps
Stworzyć pliki: pl_userdicdet.doc, pl_userdicind.doc, pl_userreq.doc i skopiować

cp pl_userdicdet.doc pl_userdicind.doc pl_userreq.doc /usr/local/mount/cafe/data/ ca_ca/req/user
Stworzyć pliki: pl_serverdicdns.doc, pl_serverreq.doc i skopiować
cp pl_serverdicdns.doc pl_serverreq.doc /usr/local/mount/cafe/data/ ca_ca/req/server
Stworzyć pliki: pl_certrequest.doc, pl_declaration.doc i skopiować
cp pl_certrequest.doc pl_declaration.doc /usr/local/mount/cafe/data/ ca_ca/req/ca
Powyższe pliki można zapisać w innych formatach, wg własnego uznania.
Stworzyć pliki: pl_main.inc, pl_title.inc, pl_main.base, pl_skel.base we wszy stkich katalogach, w których są ich odpowiedniki it_* lub en_*
Odwołania do plików it_* zamienić na pl_*
W skryptach zmienne ‘it’ zamienić na ‘pl’
UWAGA!!!

Nie tłumaczyć napisu ‘SHOW’ na przycisku (jest on wykorzystany w skryptach)
Dodać sekcje pl_* i wyedytować zmienne w pliku config (tam gdzie są it_* i en_*) wg własnych potrzeb
Dodać sekcje pl_* w pliku install.openssl.base (tam gdzie są it_* i en_*)
Dodać sekcje pl_* w pliku Makefile (tam gdzie są it_* i en_*)

- **Instalacja CAFE**

cd /usr/local/mount/cafe_src/cafe-2.1.3a-ldap-test_softu
make clean
make
make install_openssl

- **Katalog źródłowy CABE**

cd /home/ca_ca/camr-2.1.3b-test_softu

- **Edycja pliku konfiguracyjnego CABE**

cd /home/ca_ca/camr-2.1.3b-test_softu/
vim config
s/%CA_DN%/CN=CA EuroPKI, O=CA, C=PL/g
s/%CA_SERVER_NAME%/ca.europki.pl/g
s/%CA_SERVER_ADM_MAIL%/europki@ca.pl/g
s/%USER_DIR%/home/g
s/%USER%/ca_ca/g
s/%CANAME%/ca_ca/g
s/%CA_PASSW%/qwerty/g
s/%RAND_FILE%/\/dev\/random/g
s/%PORT%/7777/g
s/%SHELL_PATH%/\/bin\/sh/g
s/%PERL_PATH%/\/usr\/bin\/perl/g
s/%APACHE_PATH%/\/home\/ca_ca\/apache\/bin/g
s/%OPENSSL_PATH%/\/usr\/bin/g
s/%MTOOLS_PATH%/\/usr\/bin/g

- **Edycja openssl.cnf**

cd /home/ca_ca/camr-2.1.3b-test_softu/openssl
vim openssl.cnf.base
#--- Extensions
#--- Netscape certificate comment CPS
#nsComment="Issued under policies:\012 #http://www.europki.org/ca/root/cps/1.1/\012
#http://www.europki.org/ca/it/cps/1.1/\012 http://ca.polito.it/cps/2.1/"
nsComment="Issued under policies:\012 http://www.europki.org/ca/root/cps/1.1/\012
http://www.europki.pl/polish_ca/cps/en_cp.pdf/\012 http://ca.europki.pl/ca_ca/cps/en_cp.pdf/"
###block-names=clientSsl,email,objsign,sslCA,emailCA,objCA,serverSSL
###nsCertType =
#--- This stuff is for subjectAltName and issuerAltname.
###subjectAltName=@sub_alt_name_sec
#--- Copy subject details
issuerAltName=issuer:copy
#nsCaRevocationUrl = http://www.domain.dom/ca-crl.pem
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl

#nsCaPolicyUrl
#nsSslServerName
#--- CRL distribution points
#crlDistributionPoints=URI:http://ca.polito
crlDistributionPoints=URI:http://www.europki.pl/polish_ca/crl/crl.crl
#--- Authority Info Access
#authorityInfoAccess = OCSP;URI:http://ocsp.my.host/
#authorityInfoAccess = OCSP;URI:http://casper.wcss.wroc.pl/
#--- Certificate Policies
certificatePolicies= @polsect1,@polsect2,@polsect3
###sub_alt_name_sec
####RFC822####
####OTHER_NAME####
####DNS_NAME####
####IP_ADDRESS####
[polsect1]
policyIdentifier = 1.3.6.1.4.1.5255.1.1.1
CPS.1="http://www.europki.org/ca/root/cps/1.1/"
[polsect2]
policyIdentifier = 1.3.6.1.4.1.5255.5.1.1
#CPS.1="http://www.europki.org/ca/it/cps/1.1/
CPS.1="http://www.europki.pl/polish_ca/cps/"
[polsect3]
policyIdentifier = 1.3.6.1.4.1.5255.5.2.1
#CPS.1="http://www.europki.org/ca/it/cps/1.1/
CPS.1="http://ca.europki.pl/ca_ca/cps/"

UWAGA!!!

Identyfikator polityki zostanie przyznany w trakcie certyfikacji.
Może być to numer podrzędny do numeru Polskiego Centrum Certyfikacji EuroPKI
(np. PolicyIdentifier = 1.3.6.1.4.1.5255.5.2.1)
albo inny, przyznany CAowi przez organizacje IANA (http://www.iana.org)

- **Tłumaczenie CABE**

Aplikacja CA Manager jest jednojęzykowa, proponujemy zostać przy wersji angielskiej (przetłumaczonej przez Polskie Centrum Certyfikacji EuroPKI).
Planujemy przekonać stronę włoską o udostępnianiu nowych wersji od razu po angielsku.
Do tego czasu, w przypadku uaktualnienia trzeba tłumaczyć wszelkie makaronizmy w plikach CA Managera.
Pliki, których standardowo nie ma i trzeba je utworzyć to: en_phrase.pl, en_cred.pro.

- **Instalacja CABE**

cd /home/ca_ca/camr-2.1.3b-test_softu/
make clean
make
make install_openssl

- **Skopiowanie klucza prywatnego CA na CABE do odpowiedniego katalogu CA Managera**

cp /root/certyfikaty/CA_EuroPKI/klucz.pem /home/ca_ca/openssl/ca_ca/private/cakey.pem
chown ca_ca:ca_ca /home/ca_ca/openssl/ca_ca/private/cakey.pem

- **Skopiowanie certyfikatu CA z CAFE na CABE**

mcopy /root/certyfikaty/CA_EuroPKI/ca_cert.pem a: (na CAFE)

mcopy a:ca_cert.pem /home/ca_ca/openssl/ca_ca/cacerts/cacert.pem (na CABE)

–**Skopiowanie łańcucha certyfikatów (konkatenacji) na CAFE dla serwera apache**

cp /root/certyfikaty/CA_EuroPKI/chain.crt /usr/local/mount/httpsd/conf/ssl.crt/

–**Skopiowanie łańcucha certyfikatów (p7b i cer) na stronę WWW CA EuroPKI**

cp /root/certyfikaty/CA_EuroPKI/ca_chain.p7b /usr/local/mount/cafe/data/ca_ca/ca_cert/

cp /root/certyfikaty/CA_EuroPKI/ca_chain.cer /usr/local/mount/cafe/data/ca_ca/ca_cert/

–**Skopiowanie certyfikatów centrum w rożnych formatach na stronę WWW CA EuroPKI**

cd /root/certyfikaty/CA_EuroPKI/

cp ca_cert.txt ca_cert.pem ca_cert.der /usr/local/mount/cafe/data/ca_ca/ca_cert/

–**Katalog pomocniczego (tymczasowego) certyfikatu RA**

cd /usr/mount/cafe_src/cafe-2.1.3a-ldap-test_softu/test.openssl/ssl.crt/

UWAGA:

W wersji wloskiej w tym katalogu znajduje sie tylko tymczasowy certyfikat cacert.pem. Nie jest on nam potrzebny.Jako pomocniczy certyfikat RA i serwera apache można wtedy uzyc tego samego certyfikatu, utworzonego w trakcie kompilacji serwera apache (patrz punt 1) poprzez " make certificate".

–**Skopiowanie pomocniczego (tymczasowego) certyfikatu RA na CAFE**

cp racert.pem /usr/local/mount/cafe/data-sec/crtkeys.ssl

–**Skopiowanie pomocniczego (tymczasowego) klucza prywatnego RA z CAFE na CABE**

mcopy /usr/mount/cafe_src/cafe-2.1.3a-ldap-test_softu/test.openssl/ssl.key/rakey.pem a: (CAFE)

mcopy a:/rakey.pem /home/ca_ca/openssl/ca_ca/private/

–**Katalog pomocniczego (tymczasowego) certyfikatu serwera CAFE**

cd /usr/mount/cafe_src/cafe-2.1.3a-ldap-test_softu/test.openssl/ssl.crt/

–**Skopiowanie pomocniczego (tymczasowego) certyfikatu serwera apache na CAFE**

cp ca.europki.pl_cert.pem /usr/local/mount/httpsd/conf/ssl.crt/

–**Skopiowanie pomocniczego (tymczasowego) klucza prywatnego serwera apache na CAFE**

cp ../ssl.key/ca.europki.pl_key.pem /usr/local/httpsd/conf/ssl.key/

–**Start CAFE**

/usr/local/mount/httpd/./apachectl start

/usr/local/mount/httpsd/./apachesctl start

–**Sprawdzenie działania CAFE**

ps ax | grep httpd

```
3210 ?      S    0:01 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
3215 ?      S    0:00 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
3217 ?      S    0:00 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
3218 ?      S    0:00 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
3219 ?      S    0:00 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
3220 ?      S    0:00 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
9477 ?      S    0:01 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
9481 ?      S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
9482 ?      S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
9483 ?      S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
9484 ?      S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
9486 ?      S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
14639 ?     S    0:00 /usr/local/mount/apache/bin/httpd -DSSL -d /usr/local/mount/httpsd
24113 ?     S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
24114 ?     S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/httpd
24115 ?     S    0:00 /usr/local/mount/apache/bin/httpd -d /usr/local/mount/http
1577 pts/0  S    0:00 grep httpdd
```

- **Start CABE**

cd /home/ca_ca/gui/

./startCAGUI

- **Sprawdzenie działania CABE**

netscape http://localhost:7777

- **Generacja CRL**

Jak w punkcie 6.1. Instrukcji codziennych procedur obsługi.

- **Publikacja CRL**

Jak w punkcie 6.2. Instrukcji codziennych procedur obsługi.

- **Katalog certyfikatu RA**

mkdir /root/certyfikaty/RAserwer

cd /root/certyfikaty/RAserwer/

cp /etc/ssl/openssl.cnf .

- **Edycja pliku konfiguracyjnego openssl.cnf dla zlecenia certyfikacji RA**

vim /root/certyfikaty/RAserwer/openssl.cnf

```
[ req_distinguished_name ]
countryName                 = Country Name (2 letter code)
countryName_default         = PL
countryName_min             = 2
countryName_max             = 2
0.organizationName          = Organization Name (eg, company)
0.organizationName_default  = CA
commonName                  = Common Name (eg, YOUR name)
commonName_max              = 64
commonName_default          = RAserwer
[ req_attributes ]
#challengePassword          = A challenge password
#challengePassword_min      = 4
#challengePassword_max      = 20
#unstructuredName           = An optional company name
```

- **Generacja klucza prywatnego i zlecenia certyfikacji RA**

cd /root/certyfikaty/RAserwer/

openssl req -nodes -config openssl.cnf -new -keyout klucz.pem -out zlecenie.pem

- **Wystawienie certyfikatu dla RA**

Wkleić zawartość pliku zlecenie.pem na CAFE.

W przeglądarce otworzyć stronę https://ca.europki.pl/ca_ca/ap/pl_index.html i

w polu "Wniosek o certyfikat:" wkleić zawartość pliku zlecenie.pem.

W polu "E-mail administratora serwera:" wpisać e-mail i kliknąć przycisk dalej, obejrzeć zawartość zlecenia i jeszcze raz potwierdzić.

Podpisać zlecenie zgodnie z punktem instrukcja "obsluga"

- **Publikacja certyfikatu dla RA**

Opublikować certyfikat zgodnie z punktem ? instrukcja "obsluga"

- **Skopiowanie klucza prywatnego RA na CABE do odpowiedniego katalogu CA Managera**

cp /root/certyfikaty/RAserwer/klucz.pem /home/ca_ca/openssl/ca_ca/private/rakey.pem

- **Skopiowanie certyfikatu RA do odpowiedniego katalogu CAFE**

cp /usr/local/mount/cafe/data/ca_ca/certs/server/00000001.pem /usr/local/mount/data-sec/crtkeys.ssl/racert.pem

- **Katalog certyfikatu SSL serwera apache CAFE**

mkdir /root/certyfikaty/ca.europki.pl_serwer/
cd /root/certyfikaty/ca.europki.pl_serwer/
cp /etc/ssl/openssl.cnf .

- **Edycja pliku konfiguracyjnego openssl.cnf dla zlecenia certyfikacji serwera CAFE**

vim /root/certyfikaty/ca.europki.pl_serwer/openssl.cnf
[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = PL
countryName_min = 2
countryName_max = 2
0.organizationName = Organization Name (eg, company)
0.organizationName_default = CA
commonName = Common Name (eg, YOUR name)
commonName_max = 64
commonName_default = ca.europki.pl
[req_attributes]
#challengePassword = A challenge password
#challengePassword_min = 4
#challengePassword_max = 20
#unstructuredName = An optional company name

- **Generacja klucza prywatnego i zlecenia certyfikacji serwera CAFE**

cd /root/certyfikaty/ca.europki.pl_serwer/
openssl req -nodes -config openssl_server.cnf -new -keyout klucz.pem -out zlecenie.pem

- **Wystawienie certyfikatu dla serwera CAFE**

Wkleić zawartość pliku zlecenie.pem na CAFE.
W przeglądarce otworzyć stronę https://ca.europki.pl/ca_ca/ap/pl_index.html i
w polu "Wniosek o certyfikat:" wkleić zawartość pliku zlecenie.pem.
W polu "E-mail administratora serwera:" wpisać e-mail i kliknąć przycisk dalej, obejrzeć zawartość zlecenia i jeszcze raz potwierdzić.
Podpisać zlecenie zgodnie z punktem 3.2. Instrukcji codziennych procedur obsługi.

- **Publikacja certyfikatu dla serwera CAFE**

Opublikować certyfikat zgodnie z punktem 3.3. Instrukcji codziennych procedur obsługi.

- **Skopiowanie klucza prywatnego serwera ca.europki.pl na CAFE**

mcopy /root/certyfikaty/ca.europki.pl_serwer/klucz.pem a: (CABE)
mcopy a:/klucz.pem /usr/local/mount/httpsd/conf/ssl.key/ca.europki.pl_key.pem

- **Skopiowanie certyfikatu serwera ca.europki.pl w odpowiednie miejsce na CAFE**

cp /usr/local/mount/cafe/data/ca_ca/certs/server/00000002.pem
/usr/local/mount/httpsd/conf/ssl.cert/ca.europki.pl_cert.pem

- **Restart CAFE**

/usr/local/httpd/./apachectl restart
/usr/local/httpsd/./apachesctl restart

W przypadku problemów, pytań lub wątpliwości prosimy o kontakt pod naszymi adresami e-mail. Życzymy powodzenia w rozwijaniu EuroPKI!

Co zrobić jesli coś nie działa ?

- Jesli nie daje się złożyć zlecenia certyfikacji na CABE, sprawdzic czy apache nasluchuje na portach 80, 443,

4430

```
# netstat  -l -p | grep httpd
tcp        0      0 *:4430                  *:*                     LISTEN      12535/httpd
tcp        0      0 *:http                  *:*                     LISTEN      31041/httpd
tcp        0      0 *:https                 *:*                     LISTEN      12535/httpd
```

2.Jesli nie dziala odnawianie/uniewaznianie certyfikatu, i wyskakuje blad "Certyfikat wystawiony przez inny urzad", a jestesmy pewni, ze certyfikat jest poprawny, nalezy sprawdzi c czy apache rzeczywiscie eksportuje zmienne ssl-owe. Najlepiej uzyc do tego skryptu printenv.pl i waznego certyfikatu wystawionego przez dane
CA. Skrypt printenv.pl nalezy umiescic w katalogu /usr/local/cafe/cgi -bin-sec/

```
#!/usr/bin/perl
##
##  printenv -- demo CGI program which just prints its environment
##

print "Content-type: text/plain\n\n";
foreach $var (sort(keys(%ENV))) {
    $val = $ENV{$var};
    $val =~ s|\n|\\n|g;
    $val =~ s|"|\\"|g;
    print "${var}=\"${val}\"\n";
}
```

Zmienne ssl-we sprawdzamy poprzez wywolanie skryptu w przegladarce https://casper.wcss.wroc.pl:4430/cgi-bin/printenv.pl. (UWAGA: trzeba mic wazny certyfikat osobisty).
Pownnismy uzyskac wyswietlenie eksportowanych zmiennych, dla nas istotne to zmienne zwiazanych z certyfikatem klienta SSL_CLIENT_CERT, SSL_CLIENT_CERT_END,
SSL_CLIENT_CERT_SERIAL, SSL_CLIENT_CERT_START,
SSL_CLIENT_CN, SSL_CLIENT_DN, SSL_CLIENT_IC, SSL_CLIENT_ICN, SSL_CLIENT_IDN, SS L_CLIENT_IO,
SSL_CLIENT_IOU, SSL_CLIENT_KEY_ALGORITHM,SSL_CLIENT_KEY_EXP,
SSL_CLIENT_KEY_SIZE,SSL_CLIENT_O,SSL_CLIENT_OU,SSL_CLIENT_SIGNATURE_ALGORITHM.

Ponizej wszystkie eksportowane zmienne:

```
DOCUMENT_ROOT="/usr/local/cafe/data-sec"
GATEWAY_INTERFACE="CGI/1.1"
HTTPS="on"
HTTPS_CIPHER="RC4-MD5"
HTTPS_EXPORT="false"
HTTPS_KEYSIZE="128"
HTTPS_SECRETKEYSIZE="128"
HTTP_ACCEPT="image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*"
HTTP_ACCEPT_CHARSET="iso-8859-1,*,utf-8"
HTTP_ACCEPT_ENCODING="gzip"
HTTP_ACCEPT_LANGUAGE="en"
HTTP_CONNECTION="Keep-Alive"
```

HTTP_HOST="casper.wcss.wroc.pl:4430"
HTTP_USER_AGENT="Mozilla/4.77 [en] (X11; U; Linux 2.4.18-wolk3.6 i686)"
PATH="/sbin:/bin:/usr/sbin:/usr/bin:/usr/bin/X11:/usr/local/sbin:/usr/local/bin"
QUERY_STRING=""
REMOTE_ADDR="156.17.5.105"
REMOTE_PORT="8436"
REQUEST_METHOD="GET"
REQUEST_URI="/cgi-bin/printenv.pl"
SCRIPT_FILENAME="/usr/local/cafe/cgi-bin-sec/printenv.pl"
SCRIPT_NAME="/cgi-bin/printenv.pl"
SERVER_ADDR="156.17.5.105"
SERVER_ADMIN="test_ca@casper.wcss.wroc.pl"
SERVER_NAME="casper.wcss.wroc.pl"
SERVER_PORT="4430"
SERVER_PROTOCOL="HTTP/1.0"
SERVER_SIGNATURE="<ADDRESS>Apache/1.3.22 Server at casper.wcss.wroc.pl Port 4430</ADDRESS> \n"
SERVER_SOFTWARE="Apache/1.3.22 (Unix) mod_ssl/2.8.5 OpenSSL/0.9.6b"
SSLEAY_VERSION="OpenSSL/0.9.6b"
SSL_CLIENT_C="US"
SSL_CLIENT_CERT="-----BEGIN CERTIFICATE-----
\nMIIFUzCCBDugAwIBAgIBEzANBgkqhkiG9w0BAQQFADB5MQswCQYDVQQGEwJQTDEg\nMB4GA1UEChMXUG9sa
XRlY2huaWthIFdyb2NsYXdza2ExNjA0BgNVBAsTLVdyb2Ns\nYXdza2llIENlbnRydW0gU2llY2lvd28tU3VwZXJrb21wd
XRlcm93ZTEQMA4GA1UE\nAxMHVGVzdCBDQTAeFw0wMjEwMDExMjAwMDBaFw0wMjEyMzAxMjAwMDBaMH8xCz
AJ\nBgNVBAYTAlVTMSAwHgYDVQQKExdQb2xpdGVjaG5pa2EgV3JvY2xhd3NrYTE2MDQG\nA1UECxMtV3JvY2xhd3
NraWUgQ2VudHJ1bSBTaWVjaW93by1TdXBlcmtvbXB1dGVy\nb3dlMRYwFAYDVQQDEw1Ub21hc3ogIEtvd2FsMIGf
MA0GCSqGSIb3DQEBAQUAA4GN\nADCBiQKBgQC58Z35GSV15SbLHy4n5eTLegPXdQMXYX11PThxHffZnYIEjgJqd
SA3\nvOcIJkeEc0Fm+E0PgBIvBRUop5xODcus7A9a+3Uhi4Dwnb2jUUQt2EQ7HrxuKtkb\nKIjkpiMGCJgD9G3fhXhz
NezRamGpDoHIwegeOAZPRTfZ9/OkvHwYMQIDAQABo4IC\nYjCCAl4wDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQ
UEo9OiGS4HnY21lDIPIeKEs1D\nW5YwHwYDVR0jBBgwFoAUITWonjx8oZ9A8Zhea6kDmVhInDowDgYDVR0PAQH/
BAQD\nAgTwMIGwBglghkgBhvhCAQ0EgaIWgZ9Jc3N1ZWQgdW5kZXIgcG9saWNpZXM6MDEy\nIGh0dHA6Ly93d3
cuZXVyb3BraS5vcmcvY2Evcm9vdC9jcHMvMS4xLzAxMiBodHRw\nOi8vd3d3LmV1cm9wa2kub3JnL2NhL2l0L2Nwc
y8xLjEvMDEyIGh0dHA6Ly9jYXNw\nZXIud2Nzcy53cm9jLnBsL3Rlc3RfY2EvY3BzL2VuX2NwLnBkZi8wEQYJYIZIAYb
4\nQgEBBAQDAgWgMB0GA1UdEQQWMBSBEmJpZ3RvbUBwd3Iud3JvYy5wbDA/BgNVHR8E\nODA2MDSgMqAwhi
5odHRwOi8vY2FzcGVyLndjc3Mud3JvYy5wbC90ZXN0X2NhL2Ny\nbC9jcmwuY3JsMDcGCCsGAQUFBwEBBCswKTA
nBggrBgEFBQcwAYYbaHR0cDovL2Nh\nc3Blci53Y3NzLndyb2MucGwvMIGeBgNVHSAEgZYwgZMwQwYKKwYBBAGp
BwEBATA1\nMDMGCCsGAQUFBwIBFidodHRwOi8vd3d3LmV1cm9wa2kub3JnL2NhL3Jvb3QvY3Bz\nLzEuMS8wTAY
KKwYBBAGpBwIBATA+MDwGCCsGAQUFBwIBFjBodHRwOi8vY2FzcGVy\nLndjc3Mud3JvYy5wbC90ZXN0X2NhL2N
wcy9lbl9jcC5wZGYwDQYJKoZIhvcNAQEE\nBQADggEBADwmmUd9VXdA3HQyg8KN3tz99+lge1MDQMTW6zyJTGa
8xh1iIgfHlaip\nhHkmbZI2rb6yvc4UYJPvQbOv7x4I0X8xrTWFQvNE/WQQXnx6aC8WTW88DW2v1zwg\nmAeZDP+
q+Y/bKSGntgqYS6Fcp8+jIwEBlk4qWkj//6kaBfF7YgSAY2gG7IADFnS9\nPHNyvL6RyfX+JLzRgcG5IYTzHD4Zhn6w
DKH8jHMbRKrZXnF+h2tuLSzNcMikbpwt\nsr44eKiQKqraLIPAWFrIdgud5+zOrQsZZc3fqEm6E6wF+9yFZROU04xa
yUt0vBf6\nbahSYY1yv346Y+WrFczhCTgWbu1B1VM=\n-----END CERTIFICATE-----\n"
SSL_CLIENT_CERTIFICATE="-----BEGIN CERTIFICATE-----
\nMIIFUzCCBDugAwIBAgIBEzANBgkqhkiG9w0BAQQFADB5MQswCQYDVQQGEwJQTDEg\nMB4GA1UEChMXUG9sa
XRlY2huaWthIFdyb2NsYXdza2ExNjA0BgNVBAsTLVdyb2Ns\nYXdza2llIENlbnRydW0gU2llY2lvd28tU3VwZXJrb21wd
XRlcm93ZTEQMA4GA1UE\nAxMHVGVzdCBDQTAeFw0wMjEwMDExMjAwMDBaFw0wMjEyMzAxMjAwMDBaMH8xCz
AJ\nBgNVBAYTAlVTMSAwHgYDVQQKExdQb2xpdGVjaG5pa2EgV3JvY2xhd3NrYTE2MDQG\nA1UECxMtV3JvY2xhd3
NraWUgQ2VudHJ1bSBTaWVjaW93by1TdXBlcmtvbXB1dGVy\nb3dlMRYwFAYDVQQDEw1Ub21hc3ogIEtvd2FsMIGf

MA0GCSqGSIb3DQEBAQUAA4GN\nADCBiQKBgQC58Z35GSV15SbLHy4n5eTLegPXdQMXYX11PThxHffZnYIEjgJqd
SA3\nvOcIJkeEc0Fm+E0PgBIvBRUop5xODcus7A9a+3Uhi4Dwnb2jUUQt2EQ7HrxuKtkb\nKIjkpiMGCJgD9G3fhXhz
NezRamGpDoHIwegeOAZPRTfZ9/OkvHwYMQIDAQABo4IC\nYjCCAl4wDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQ
UEo9OiGS4HnY21lDIPIeKEs1D\nW5YwHwYDVR0jBBgwFoAUITWonjx8oZ9A8Zhea6kDmVhInDowDgYDVR0PAQH/
BAQD\nAgTwMIGwBglghkgBhvhCAQ0EgaIWgZ9Jc3N1ZWQgdW5kZXIgcG9saWNpZXM6MDEy\nIGh0dHA6Ly93d3
cuZXVyb3BraS5vcmcvY2Evcm9vdC9jcHMvMS4xLzAxMiBodHRw\nOi8vd3d3LmV1cm9wa2kub3JnL2NhL2l0L2Nwc
y8xLjEvMDEyIGh0dHA6Ly9jYXNw\nZXIud2Nzcy53cm9jLnBsL3Rlc3RfY2EvY3BzL2VuX2NwLnBkZi8wEQYJYIZIAYb
4\nQgEBBAQDAgWgMB0GA1UdEQQWMBSBEmJpZ3RvbUBwd3Iud3JvYy5wbDA/BgNVHR8E\nODA2MDSgMqAwhi
5odHRwOi8vY2FzcGVyLndjc3Mud3JvYy5wbC90ZXN0X2NhL2Ny\nbC9jcmwuY3JsMDcGCCsGAQUFBwEBBCswKTA
nBggrBgEFBQcwAYYbaHR0cDovL2Nh\nc3Blci53Y3NzLndyb2MucGwvMIGeBgNVHSAEgZYwgZMwQwYKKwYBBAGp
BwEBATA1\nMDMGCCsGAQUFBwIBFidodHRwOi8vd3d3LmV1cm9wa2kub3JnL2NhL3Jvb3QvY3Bz\nLzEuMS8wTAY
KKwYBBAGpBwIBATA+MDwGCCsGAQUFBwIBFjBodHRwOi8vY2FzcGVy\nLndjc3Mud3JvYy5wbC90ZXN0X2NhL2N
wcy9lbl9jcC5wZGYwDQYJKoZIhvcNAQEE\nBQADggEBADwmmUd9VXdA3HQyg8KN3tz99+lge1MDQMTW6zyJTGa
8xh1iIgfHlaip\nhHkmbZI2rb6yvc4UYJPvQbOv7x4I0X8xrTWFQvNE/WQQXnx6aC8WTW88DW2v1zwg\nmAeZDP+
q+Y/bKSGntgqYS6Fcp8+jIwEBlk4qWkj//6kaBfF7YgSAY2gG7IADFnS9\nPHNyvL6RyfX+JLzRgcG5IYTzHD4Zhn6w
DKH8jHMbRKrZXnF+h2tuLSzNcMikbpwt\nsr44eKiQKqraLIPAWFrIdgud5+zOrQsZZc3fqEm6E6wF+9yFZROU04xa
yUt0vBf6\nbahSYY1yv346Y+WrFczhCTgWbu1B1VM=\n-----END CERTIFICATE-----\n"
SSL_CLIENT_CERT_END="Dec 30 12:00:00 2002 GMT"
SSL_CLIENT_CERT_SERIAL="13"
SSL_CLIENT_CERT_START="Oct 1 12:00:00 2002 GMT"
SSL_CLIENT_CN="Tomasz Kowal"
SSL_CLIENT_DN="/C=US/O=Politechnika Wroclawska/OU=Wroclawskie Centrum Sieciowo -
Superkomputerowe/CN=Tomasz Kowal"
SSL_CLIENT_IC="PL"
SSL_CLIENT_ICN="Test CA"
SSL_CLIENT_IDN="/C=PL/O=Politechnika Wroclawska/OU=Wroclawskie C entrum Sieciowo -
Superkomputerowe/CN=Test CA"
SSL_CLIENT_IO="Politechnika Wroclawska"
SSL_CLIENT_IOU="Wroclawskie Centrum Sieciowo -Superkomputerowe"
SSL_CLIENT_KEY_ALGORITHM="Not supported by mod_ssl"
SSL_CLIENT_KEY_EXP="Not supported by mod_ssl"
SSL_CLIENT_KEY_SIZE="Not supported by mod_ssl"
SSL_CLIENT_O="Politechnika Wroclawska"
SSL_CLIENT_OU="Wroclawskie Centrum Sieciowo -Superkomputerowe"
SSL_CLIENT_SIGNATURE_ALGORITHM="md5WithRSAEncryption"
SSL_EXPORT="false"
SSL_KEYSIZE="128"
SSL_PROTOCOL_VERSION="SSLv3"
SSL_SECRETKEYSIZE="128"
SSL_SERVER_C="PL"
SSL_SERVER_CERT="-----BEGIN CERTIFICATE-----
\nMIIFYzCCBEugAwIBAgIBAjANBgkqhkiG9w0BAQQFADB5MQswCQYDVQQGEwJQTDEg\nMB4GA1UEChMXUG9sa
XRlY2huaWthIFdyb2NsYXdza2ExNjA0BgNVBAsTLVdyb2Ns\nYXdza2llIENlbnRydW0gU2llY2lvd28tU3VwZXJrb21wd
XRlcm93ZTEQMA4GA1UE\nAxMHVGVzdCBDQTAeFw0wMjA3MTIxMzAwMDBaFw0wMjEyMzAxMjAwMDBaMIGFMQs
w\nCQYDVQQGEwJQTDEgMB4GA1UEChMXUG9saXRlY2huaWthIFdyb2NsYXdza2ExNjA0\nBgNVBAsTLVdyb2NsYX
dza2llIENlbnRydW0gU2llY2lvd28tU3VwZXJrb21wdXRl\ncm93ZTEcMBoGA1UEAxMTY2FzcGVyLndjc3Mud3JvYy5w
bDCBnzANBgkqhkiG9w0B\nAQEFAAOBjQAwgYkCgYEAu/ZCgk1fSGXonU0MH3AMdpdENALWBE/l8EPlzWdXy6ma\
nwNB72OunLL+1I8T3Rte2v4MO3NSVoapTXRkeA2Jmddo4FG23EX7eN8MG6StNnD5e\nKLayqPAhB+UcOejOF29N

UU6ZFem9qOi5DUU1EvjLtqB9uk9YiF4l+wVAdCoLo8cC\nAwEAAaOCAmswggJnMAwGA1UdEwEB/wQCMAAwHQYD
VR0OBBYEFDpTtopom1Y8Wk+1\n025XKyWQW8RVMB8GA1UdIwQYMBaAFCE1qJ48fKGfQPGYXmupA5lYSJw6MA8
GA1Ud\nDwEB/wQFAwMH/4AwgbAGCWCGSAGG+EIBDQSBohaBn0lzc3VlZCB1bmRlciBwb2xp\nY2llczowMTIgaHR
0cDovL3d3dy5ldXJvcGtpLm9yZy9jYS9yb290L2Nwcy8xLjEv\nMDEyIGh0dHA6Ly93d3cuZXVyb3BraS5vcmcvY2Ev
aXQvY3BzLzEuMS8wMTIgaHR0\ncDovL2Nhc3Blci53Y3NzLndyb2MucGwvdGVzdF9jYS9jcHMvZW5fY3AucGRmLzA
R\nBglghkgBhvhCAQEEBAMCBkAwJQYDVR0RBB4wHIEaYmlndG9tQGNhc3Blci53Y3Nz\nLndyb2MucGwwPwYDVR0
fBDgwNjA0oDKgMIYuaHR0cDovL2Nhc3Blci53Y3NzLndy\nb2MucGwvdGVzdF9jYS9jcmwvY3JsLmNybDA3BggrBgE
FBQcBAQQrMCkwJwYIKwYB\nBQUHMAGGG2h0dHA6Ly9jYXNwZXIud2Nzcy53cm9jLnBsLzCBngYDVR0gBIGWMIG
T\nMEMGCisGAQQBqQcBAQEwNTAzBggrBgEFBQcCARYnaHR0cDovL3d3dy5ldXJvcGtp\nLm9yZy9jYS9yb290L2Nw
cy8xLjEvMEwGCisGAQQBqQcCAQEwPjA8BggrBgEFBQcC\nARYwaHR0cDovL2Nhc3Blci53Y3NzLndyb2MucGwvdGV
zdF9jYS9jcHMvZW5fY3Au\ncGRmMA0GCSqGSIb3DQEBBAUAA4IBAQAoAx0fUc8pIDcDDNbJHfo05jRoIpRASsNZ\n
8jmqGtYmfA4o5wuh8NM4XDJ4UxYoUvnHaEUkK+LIXjLw29zi6UpwKQB2gzCLmN5X\nxfuJ9fz1ytH/4jtq2e1ygeN/Z
Bcxv+ftgxVpGApYI/A6oC6ANB+7IOD/5wf+BUk8\n6bD3BI3E0Fee8jpFeDM5jSQvCFgW+FpLXOstBc87dFZ9znrffO
j5pSEKbbncocWL\nPTuNmDtqKROetMVXQ9wTkzRq+qNzigIVymzf9GyLRqPdut/Ari3jiJWg+F/iyJMD\nRENoXfa7e9
4Nd8m5HystNAY2KKIjBKakVbl9FS3jLNf/LzFEjtFE\n-----END CERTIFICATE-----\n"
SSL_SERVER_CERTFILE="Not supported by mod_ssl"
SSL_SERVER_CERTIFICATE="-----BEGIN CERTIFICATE-----
\nMIIFYzCCBEugAwIBAgIBAjANBgkqhkiG9w0BAQQFADB5MQswCQYDVQQGEwJQTDEg\nMB4GA1UEChMXUG9sa
XRlY2huaWthIFdyb2NsYXdza2ExNjA0BgNVBAsTLVdyb2Ns\nYXdza2llIENlbnRydW0gU2llY2lvd28tU3VwZXJrb21wd
XRlcm93ZTEQMA4GA1UE\nAxMHVGVzdCBDQTAeFw0wMjA3MTIxMzAwMDBaFw0wMjEyMzAxMjAwMDBaMIGFMQs
w\nCQYDVQQGEwJQTDEgMB4GA1UEChMXUG9saXRlY2huaWthIFdyb2NsYXdza2ExNjA0\nBgNVBAsTLVdyb2NsYX
dza2llIENlbnRydW0gU2llY2lvd28tU3VwZXJrb21wdXRl\ncm93ZTEcMBoGA1UEAxMTY2FzcGVyLndjc3Mud3JvYy5w
bDCBnzANBgkqhkiG9w0B\nAQEFAAOBjQAwgYkCgYEAu/ZCgk1fSGXonU0MH3AMdpdENALWBE/l8EPlzWdXy6ma\
nwNB72OunLL+1I8T3Rte2v4MO3NSVoapTXRkeA2Jmddo4FG23EX7eN8MG6StNnD5e\nKLayqPAhB+UcOejOF29N
UU6ZFem9qOi5DUU1EvjLtqB9uk9YiF4l+wVAdCoLo8cC\nAwEAAaOCAmswggJnMAwGA1UdEwEB/wQCMAA wHQYD
VR0OBBYEFDpTtopom1Y8Wk+1\n025XKyWQW8RVMB8GA1UdIwQYMBaAFCE1qJ48fKGfQPGYXmupA5lYSJw6MA8
GA1Ud\nDwEB/wQFAwMH/4AwgbAGCWCGSAGG+EIBDQSBohaBn0lzc3VlZCB1bmRlciBwb2xp\nY2llczowMTIgaHR
0cDovL3d3dy5ldXJvcGtpLm9yZy9jYS9yb290L2Nwcy8xLjEv\nMDEyIGh0dHA6Ly93d3cuZXVyb3BraS5vcmcvY2Ev
aXQvY3BzLzEuMS8wMTIgaHR0\ncDovL2Nhc3Blci53Y3NzLndyb2MucGwvdGVzdF9jYS9jcHMvZW5fY3AucGRmLzA
R\nBglghkgBhvhCAQEEBAMCBkAwJQYDVR0RBB4wHIEaYmlndG9tQGNhc3Blci53Y3Nz\nLndyb2MucGwwPwYDVR0
fBDgwNjA0oDKgMIYuaHR0cDovL2Nhc3Blci53Y3NzLndy\nb2MucGwvdGVzdF9jYS9jcmwvY3JsLmNybDA3BggrBgE
FBQcBAQQrMCkwJwYIKwYB\nBQUHMAGGG2h0dHA6Ly9jYXNwZXIud2Nzcy53cm9jLnBsLzCBngYDVR0gBIGWMIG
T\nMEMGCisGAQQBqQcBAQEwNTAzBggrBgEFBQcCARYnaHR0cDovL3d3dy5ldXJvcGtp\nLm9yZy9jYS9yb290L2Nw
cy8xLjEvMEwGCisGAQQBqQcCAQEwPjA8BggrBgEFBQcC\nARYwaHR0cDovL2Nhc3Blci53Y3NzLndyb2MucGwvdGV
zdF9jYS9jcHMvZW5fY3Au\ncGRmMA0GCSqGSIb3DQEBBAUAA4IBAQAoAx0fUc8pIDcDDNbJHfo05jRoIpRASsNZ\n
8jmqGtYmfA4o5wuh8NM4XDJ4UxYoUvnHaEUkK+LIXjLw29zi6UpwKQB2gzCLmN5X\nxfuJ9fz1ytH/4jtq2e1ygeN/Z
Bcxv+ftgxVpGApYI/A6oC6ANB+7IOD/5wf+BUk8\n6bD3BI3E0Fee8jpFeDM5jSQvCFgW+FpLXOstBc87dFZ9znrffO
j5pSEKbbncocWL\nPTuNmDtqKROetMVXQ9wTkzRq+qNzigIVymzf9GyLRqPdut/Ari3jiJWg+F/iyJMD\nRENoXfa7e9
4Nd8m5HystNAY2KKIjBKakVbl9FS3jLNf/LzFEjtFE\n-----END CERTIFICATE-----\n"
SSL_SERVER_CERTIFICATELOGDIR="Not supported by mod_ssl"
SSL_SERVER_CERT_END="Dec 30 12:00:00 2002 GMT"
SSL_SERVER_CERT_SERIAL="02"
SSL_SERVER_CERT_START="Jul 12 13:00:00 2002 GMT"
SSL_SERVER_CN="casper.wcss.wroc.pl"
SSL_SERVER_DN="/C=PL/O=Politechnika Wroclawska/OU=Wroclawskie Centrum Sieciowo -
Superkomputerowe/CN=casper.wcss.wroc.pl"
SSL_SERVER_IC="PL"
SSL_SERVER_ICN="Test CA"

SSL_SERVER_IDN="/C=PL/O=Politechnika Wroclawska/OU=Wroclawskie Centrum Sieciowo -
Superkomputerowe/CN=Test CA"
SSL_SERVER_IO="Politechnika Wroclawska"
SSL_SERVER_IOU="Wroclawskie Centrum Sieciowo-Superkomputerowe"
SSL_SERVER_KEYFILE="Not supported by mod_ssl"
SSL_SERVER_KEYFILETYPE="Not supported by mod_ssl"
SSL_SERVER_KEY_ALGORITHM="Not supported by mod_ssl"
SSL_SERVER_KEY_EXP="Not supported by mod_ssl"
SSL_SERVER_KEY_SIZE="Not supported by mod_ssl"
SSL_SERVER_O="Politechnika Wroclawska"
SSL_SERVER_OU="Wroclawskie Centrum Sieciowo-Superkomputerowe"
SSL_SERVER_SESSIONDIR="Not supported by mod_ssl"
SSL_SERVER_SIGNATURE_ALGORITHM="md5WithRSAEncryption"
SSL_SSLEAY_VERSION="OpenSSL/0.9.6b"
SSL_STRONG_CRYPTO="Not supported by mod_ssl"

–Nie mozna wczytac zlecenia certyfikacji na CA Managaer, wygenerowanego poprzez CAFE. Zlecena certyfikacji sa szyfrowane certyfikatami CA (cacert.pem) i RA (racert.pem) , znajdujacymi sie na CAFE, w katalogu /usr/local/cafe/data-sec/crtkeys.ssl. Zlecenie odszyfrowane sa kluczami CA i RA na CABE, znajdujacymi sie w katalogu /home/ca_ca/openssl/ca_ca/private/. Jesli bedzie niezgodnosc odpowiednich certyfikatow i kluczy, to zlecenia nie da sie odszyfrowac. UWAGA: CABE ZAWSZE probuje odszyfrowywac zlecenie, nie da sie wczytac zlecenia niezaszyfrowanego.

Procedury codzinnej obsługi CA dla operatora używającego oprogramowania do prowadzenie CA: CA Front End i CA Back End.

1. Wstęp

Wszystkie opisane niżej procedury odbywają się na dwóch jednostkach: serwerze dostępowym – CA Front End – **CAFE** i jednostce podpisującej – CA Back End – **CABE**.

2. Uruchomienie CABE.

CABE:

cd /home/ca_ca/gui

./startCAGUI

name of CA: ca_ca

Jeśli CA Manager nie był prawidłowo zatrzymany, pojawi się komunikat:

View CA credentials

CN=CA EuroPKI,O=CA,C=PL

Cancel the credentials [y/n]? n

Jeśli CA Manager był prawidłowo zatrzymany, pojawi się komunikat:

Insert PIN for CA ca_ca:

Wciśnij Enter i powinien pojawić się komunikat:

CA-GUI available via port 7777

Uruchom browser i wpisz URL:

http://localhost:7777

Powinno pokazać się okno CA Managera.

3. Wydawanie certyfikatów.

3.1. Sprawdzanie zleceń certyfikacji.

CAFE:

cd /usr/local/mount/cafe/data-sec/ca_ca/reqs/newreqs/ca_ra

ls

Jan__Kowalski~9874_DATE17-10-2002_req.p7

mformat a:

mcopy Jan__Kowalski~9874_DATE17-10-2002_req.p7 a:

3.2. Podpisywanie zleceń certyfikacji.

CABE:

REQUESTS -> load -> Insert disk -> OK.

Wybierz zlecenie i kliknij Sign.

Sprawdź poprawność danych.

Ustaw datę ważności certyfikatu.

Zaznacz ustawienia:

	Basic constraints	**Select the extensions**	**Key Usage**	**Extended Key Usage**
Użytkownik indywidualny	NonCA	clientSsl, email	dataEncipherment, digitalSignature, keyEncipherment, nonRepudiation	żadne
Serwer	NonCA	serverSSL	dataEncipherment, digitalSignature, keyAgreement, keyEncipherment, nonRepudiation	żadne
CA	CA	emailCA, objsignCA, sslCA	cRLSign, dataEncipherment, digitalSignature, keyCertSign, keyEncipherment, nonRepudiation	żadne

Kliknij Sign.

Sprawdź poprawność ustawień.

Kliknij Sign.

Powinien wyświetlić się certyfikat.

Kliknij CERTIFICATES -> save -> Save to disk -> OK.

Powinien pojawić się komunikat:

Saving the certificate

xxxxxxxx_cert.pem

z odpowiednim numerem seryjnym.

Znajduje się on pod ścieżką:

a:/ca_ca/xxxxxxxx_cert.pem

3.3. Publikowanie certyfikatów.

CAFE:

Certyfikat dla użytkownika indywidualnego:
cd /usr/local/mount/cafe/data/ca_ca/certs/user
mcopy a:/ca_ca/*.pem .
perl genlist.pl
Sprawdź czy opublikowany certyfikat jest widoczny na stronie:
http://ca.europki.pl/ca_ca/certs/user

Certyfikat dla serwera:
cd /usr/local/mount/cafe/data/ca_ca/certs/server
mcopy a:/ca_ca/*.pem .
perl genlist.pl
Sprawdź czy opublikowany certyfikat jest widoczny na stronie:
http://ca.europki.pl/ca_ca/certs/server

Certyfikat dla CA:
cd /usr/local/mount/cafe/data/ca_ca/certs/ca
mcopy a:/ca_ca/*.pem .
perl genlist.pl
Sprawdź czy opublikowany certyfikat jest widoczny na stronie:
http://ca.europki.pl/ca_ca/certs/ca

Wyślij e-mail do posiadacza certyfikatu:
Został nadany Panu certyfikat CA EuroPKI o numerze seryjnym xxxxxxxx (wpisz odpowiedni numer). Certyfikat MUSI być pobrany i zainstalowany NA TYM SAMYM KOMPUTERZE I Z TEJ SAMEJ PRZEGLĄDARKI, z której wysłane było zlecenie. W celu zainstalowania proszę wejść na stronę:
http://ca.europki.pl/ca_ca/certs/ins
wpisać do okienka numer seryjny xxxxxxxx (wpisz odpowiedni numer) i kliknać „Dalej”. Po zainstalowaniu proszę sprawdzić czy certyfikat zainstalował się poprawnie.
W Internet Explorer: Narzędzia -> Opcje internetowe -> Zawartość -> Certyfikaty -> Osobisty
W Netscape 4.x: Communicator -> Narzędzia -> Informacje o ochronie -> Certyfikaty -> Twoje
W Netscape 7.x: Edit -> Preferences -> Privacy & Security -> Certificates -> Manage Certificates -> Your certificates
W przypadku problemów proszę o kontakt: europki@ca.pl lub tel. +48*******.

4. Odnawianie certyfikatów.

UWAGA!!!
Zlecenie odnowienia certyfikatu MUSI BYĆ przesłane przez posiadacza certyfikatu PRZED upływem wa żności certyfikatu, natomiast podpisanie może nastąpić dopiero PO upływie ważności certyfikatu.

4.1. Sprawdzanie zleceń odnowienia certyfikatów.

CAFE:
cd /usr/local/mount/cafe/data-sec/ca_ca/reqs/newreqs/renew
ls
Jan__Kowalski~9874_DATE17-10-2002_req.p7
mformat a:
mcopy Jan__Kowalski~9874_DATE17-10-2002_req.p7 a:

4.2. Odnawianie certyfikatów ze zlecenia.

Patrz 2.2.

4.3. Odnawianie certyfikatów bez zlecenia.

CABE:
USERS -> wybierz certyfikat -> kliknij na numer seryjny -> Renew the certificate -> w nowym oknie postępuj jak w 3.2.

4.4. Publikowanie odnowionych certyfikatów.

Patrz 3.3.

5. Unieważnianie certyfikatów.

UWAGA!!!
Po każdym unieważnieniu certyfikatu należy wygenerować i opublikować listę unieważnionych certyfikatów (CRL).

5.1. Sprawdzanie zleceń unieważnienia certyfikatów.

CAFE:
cd /usr/local/mount/cafe/data-sec/ca_ca/revoke
ls
revoke.lst
mformat a:
mcopy revoke.lst a:

5.2. Unieważnianie certyfikatów ze zlecenia.

CABE:
REVOKE -> load -> continue -> Revoke the certificate -> kliknij na przycisk „Revoke the certificate” -> Issue new CRL -> postępuj jak w 6.1.

5.3. Unieważnianie certyfikatów bez zlecenia.

CABE:

USERS -> wybierz certyfikat -> kliknij na numer seryjny -> Revoke the certificate -> kliknij na przycisk „Revoke the certificate" -> Issue new CRL -> postępuj jak w 6.1.

6. Listy unieważnionych certyfikatów (CRL).

UWAGA!!!

CRL należy generować i publikować okresowo, np. co miesiąc, nawet wtedy, gdy nie unieważniono w tym czasie żadnych certyfikatów.

6.1. Generacja CRL.

CABE:

CRL -> generate -> Wpisz datę następnej publikacji CRL i kliknij „Generate" -> OK -> Save CRL -> Save CRL to file.

UWAGA!!!

CRL jest zapisywany pod nazwą YYYYMMDDcrl.* (b64, der, pem, txt) [YYYY – rok, MM – miesiąc, DD – dzień]

Najlepiej wyczyść okienko z datą i zapisz CRL we wszystkich formatach klikając przysisk „SAVE":
Save CRL to file -> OK.
Powinien pojawić się komunikat:
Saving CRL in file format PEM
Saving CRL in file format BASE64
Saving CRL in file format TXT
Saving CRL in file format DER
Teraz zapisz listy CRL na dyskietkę:
CRL -> save -> Save to disk? -> OK.
Powinien pojawić się komuniakat:
Saving CRL
1. crl.pem
2. crl.b64
3. crl.txt
4. crl.der
Znajdują się one pod ścieżką:
a:/ca_ca/crl.*

6.2. Publikowanie CRL.

CAFE:

cd /usr/local/mount/cafe/data/ca_ca/crl
mcopy a:/ca_ca/crl.* .
Sprawdź czy listy CRL są widoczne na stronie:
http://ca.europki.pl/ca_ca/crl

7. Zatrzymanie CABE.

CABE:

Kliknij STOP w CA Managerze lub:

cd /home/ca_ca/gui

./stopCAGUI

CA GUI stopped...

8. Logi.

Podczas działania CA Managera wszelkie logi i komunikaty o błędach znajdują się pod ścieżką:

CABE:

/home/ca_ca/gui/logs

Załącznik 1 Polityka certyfikacji Polskiego Centrum Certyfikacji EuroPKI

Polityka certyfikacji Polskiego Centrum Certyfikacji EuroPKI

(CN = EuroPKI Polish Certification Authority, O = EuroPKI, C = PL)

Wersja 1.3

Styczeń 2003

OID 1.3.6.1.4.1.5255.5.1.1

Spis treści

WPROWADZENIE

Opis dokumentu

Poniższy dokument opisuje procedury stosowane przez Polskie Centrum Certyfikacji EuroPKI podczas certyfikacji klucza publicznego, definiuje uczestników tego procesu oraz określa obszary zastosowań certyfikatów uzyskanych w tym procesie. Dokument ten jest w pełni zgodny z zasadami opisanymi w „EuroPKI Certificate Policy" [1].

Polskie Centrum Certyfikacji EuroPKI powołano do życia w trakcie realizacji projektu "Building Trust in networking in Newly Associated States through the use of secure information society technologies (NASTEC)" V Programu Ramowego Unii Europejskiej.

Polskie Centrum Certyfikacji EuroPKI występuje jako nadrzędny urząd certyfikacyjny w polskiej infrastrukturze EuroPKI. Jego zadaniem jest poświadczanie swoim podpisem elektronicznym:

- kluczy publicznych należących do urzędów certyfikacyjnych podporządkowanych polskiej infrastrukturze kluczy publicznych EuroPKI;
- kluczy publicznych urzędów rejestracyjnych występujących w imieniu Polskiego Centrum Certyfikacji EuroPKI;
- kluczy publicznych użytkowników końcowych.

Certyfikaty Polskiego Centrum Certyfikacji EuroPKI wydawane są **wyłącznie** dla osób i instytucji związanych ze środowiskiem naukowo-badawczym i akademickim oraz dla osób i instytucji zainteresowanych udziałem w inicjatywie EuroPKI.

Certyfikaty Polskiego Centrum Certyfikacji EuroPKI wydawane są **wyłącznie** w celach naukowo-badawczych i edukacyjnych.

Certyfikaty Polskiego Centrum Certyfikacji EuroPKI wydawane są **wyłącznie** w celu zabezpieczenia poczty elektronicznej, serwerów WWW, serwerów SSL, uwierzytelniania stron.
Polskie Centrum Certyfikacji EuroPKI **nie jest** kwalifikowanym podmiotem swiadczącym usługi certyfikacyjne.

Podpis elektroniczny weryfikowany przy pomocy certyfikatu Polskiego Centrum Certyfikacji EuroPKI **nie wywołuje** skutków prawnych równorzędnych podpisowi własnoręcznemu.

Certyfikaty wydawane przez Polskie Centrum Certyfikacji EuroPKI są **bezpłatne**.

Polskie Centrum Certyfikacji EuroPKI nie ponosi **żadnej** odpowiedzialności za skutki użycia tych certyfikatów.

Gwarancja Polskiego Centrum Certyfikacji EuroPKI wynosi **0 zł**.

Polskie Centrum Certyfikacji EuroPKI jest prowadzone przez:
Wrocławskie Centrum Sieciowo-Superkomputerowe (WCSS)
Politechnika Wrocławska (PWR)
Wybrzeże Wyspiańskiego 27

50-370 Wrocław
Polska (PL)

Identyfikator polityki

Polityka certyfikacji Polskiego Centrum Certyfikacji EuroPKI jest identyfikowana unikatowym, zarejestrowanym identyfikatorem obiektu (OID):

1.3.6.1.4.1.5255.5.1.1

Poszczególne komponenty identyfikatora OID to:

ISO assigned	1
Organization acknowledged by ISO	3
US Department of Defence	6
Internet	1
Private	4
IANA registered private enterprises	1
EuroPKI	5255
Polish Certification Authority	5
Major version	1
Minor version	1

Środowisko działania

Polskie Centrum Certyfikacji EuroPKI świadczy usługi certyfikacji urzędów, użytkowników końcowych dla środowiska akademickiego i naukowo-badawczego oraz dla urzędów administracji zainteresowanych udziałem w inicjatywie EuroPKI.

Urzędy certyfikacyjne

Certyfikacja urzędów następuje na podstawie specjalnej umowy dwustronnej podpisanej, zgodnie z wymogami niniejszego dokumentu, przez urząd zlecający certyfikację oraz Polskie Centrum Certyfikacji EuroPKI. Umowa ta określa zakres działania urzędu podporządkowanego. Wszystkie urzędy certyfikacyjne podporządkowane Polskiemu Centrum Certyfikacji EuroPKI muszą respektować wymagania i ograniczenia narzucane Politykę Certyfikacji Polskiego Centrum Certyfikacji EuroPKI.

Zakłada się, że każdy urząd certyfikacyjny poświadczany przez Polskie Centrum Certyfikacji EuroPKI działa zgodnie z niniejszym dokumentem. Jeśli urząd zlecający certyfikację swego klucza publicznego przyjmuje te zasady, to nie musi przedstawiać własnej polityki. Jeżeli urząd certyfikacyjny zlecający certyfikację swego klucza publicznego zamierza dysponować własną polityką i/lub kodeksem postępowania certyfikacyjnego, to dokumenty te muszą zostać zatwierdzone przez jego nadrzędny urząd certyfikacyjny.

Urzędy rejestracyjne

Polskie Centrum Certyfikacji EuroPKI występuje jednocześnie jako urząd rejestracyjny. W celu usprawnienia funkcjonowania Polskie Centrum Certyfikacji EuroPKI może powoływać swoje urzędy rejestracyjne. Rolę urzędu rejestracyjnego powierza się zaufanej osobie, wskazanej przez instytucję. Osoba taka podpisuje umowę z urzędem certyfikacyjnym, w którego imieniu występuje i zobowiązuje się do przestrzegania zasad niniejszego dokumentu. Osoba wskazana do pełnienia funkcji urzędu rejestracyjnego musi zostać zatwierdzona przez

urząd certyfikacyjny, któremu służy.

Każdy urząd certyfikacyjny podporządkowany Polskiemu Centrum Certyfikacji EuroPKI może korzystać w swojej działalności z urzędów rejestracyjnych. Podporządkowany urząd certyfikacyjny może również sam pełnić rolę urzędu rejestracyjnego na zasadach opisanych powyżej.

Użytkownicy końcowi

Zgodnie z niniejszym dokumentem, użytkownikiem końcowym jest system komputerowy lub osoba ubiegająca się o certyfikat.

Obszar zastosowania

Celem przedsięwzięcia jest promowanie szerokiego stosowania certyfikatów klucza publicznego w różnych aplikacjach internetowych, głównie dla poczty elektronicznej, dostępu do WWW, zdalnego dostępu do komputerów (Telnet) i plików (FTP). Dodatkowym celem będzie zwiększenie bezpieczeństwa funkcjonowania naukowo-akademickich sieci komputerowych.

Adresy kontaktowe

Organizacja nadzorująca

Za Politykę Certyfikacji odpowiada Zespół Bezpieczeństwa Komputerowo-Sieciowego WCSS Politechniki Wrocławskiej.

Osoba kontaktowa

Osobą kontaktową jest:
Dr inż. Józef Janyszek
WCSS Politechniki Wrocławskiej
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
tel.: +48 71 3202456 / +48 71 3203921
fax: +48 71 3225797
http://www.europki.pl
e-mail: europki@pwr.wroc.pl

Osoba określająca dostosowanie Kodeksu Postępowania Certyfikacyjnego do polityki

Dr inż. Józef Janyszek
WCSS Politechniki Wrocławskiej
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
tel.: +48 71 3202456/ +48 71 3203921
fax: +48 71 3225797
http: //www.europki.pl
e-mail: europki@pwr.wroc.pl

ZASADY OGÓLNE

W tej części polityki są przedstawione zobowiązania, jakie przyjmuje na siebie każda ze stron uczestniczących w procesie certyfikacji. Ponadto ustala się zasady finansowe, poziom niezawodności usługi oraz dopuszczalne metody dystrybucji informacji związanej z procesem certyfikacji.

Obowiązki

Obowiązki urzędu certyfikacyjnego

Urząd certyfikacyjny jest odpowiedzialny za świadczenie usługi certyfikacji zgodnie z niniejszą Polityką Certyfikacji. Do jego zadań należy:

- przyjmowanie i realizacja zleceń certyfikacji;
- uwierzytelnianie jednostek ubiegających się o certyfikację (np. za pomocą odpowiedniego urzędu rejestracyjnego);
- podpisywanie umowy z urzędem nadrzędnym i respektowanie zasad tej umowy;
- podpisywanie umowy z urzędami rejestracyjnymi wspomagającymi proces uwierzytelniania;
- wystawianie certyfikatów klucza publicznego X.509 na podstawie otrzymanych zleceń;
- przekazywanie zwrotne gotowego certyfikatu zleceniodawcy oraz publikacja certyfikatu w ogólnodostępnym repozytorium;
- obsługa zleceń odwołania certyfikatów;
- utrzymywanie listy odwołanych certyfikatów;
- ochrona danych zleceniodawcy;
- przetwarzanie danych zleceniodawcy wyłącznie do celów związanych z usługami certyfikacji.

Obowiązki urzędu rejestracyjnego

Urząd rejestracyjny działa zgodnie z niniejszą polityką pełniąc usługę uwierzytelniania. Jego zadania to:

- sprawdzenie poprawności powiązania klucza publicznego z identyfikatorem jego użytkownika;
- zatwierdzenie przypisania subskrybenta danemu urzędowi certyfikacyjnemu;
- podpisywanie umów z urzędami certyfikacyjnymi, w imieniu których urząd rejestracyjny ma występować i przestrzeganie zasad umowy.

Obowiązki subskrybenta

Subskrybent, czyli podporządkowany urząd certyfikacyjny lub użytkownik końcowy zobowiązuje się przestrzegać zasad niniejszej polityki, w tym właściwie chronić swój klucz prywatny, upoważnić urząd certyfikacyjny do przetwarzania danych do celów związanych z usługami certyfikacji i występować do urzędu certyfikacyjnego o odwołanie certyfikatu, gdy zajdzie taka potrzeba.

Użytkownik końcowy nie podpisuje umowy ze swoim urzędem certyfikacyjnym ani urzędem rejestracyjnym.

Obowiązki strony ufającej certyfikatom

Strona ufająca certyfikatom jest zobowiązana do zapoznania się z niniejszą polityką przed wyciągnięciem jakichkolwiek wniosków dotyczących zaufania certyfikatowi wydanemu zgodnie z niniejszą polityką. Strona ufająca certyfikatom jest zobowiązana do sprawdzenia statusu certyfikatu przed podjęciem decyzji o zaufaniu certyfikatowi.

Obowiązki repozytorium

Urząd certyfikacyjny jest zobowiązany do utrzymywania ogólnodostępnego repozytorium do publikowania certyfikatów, list unieważnionych certyfikatów, polityki certyfikacji i kodeksu postępowania certyfikacyjnego.

Odpowiedzialność prawna

Odpowiedzialność urzędu certyfikacyjnego

Usługa certyfikacji świadczona w Polsce w ramach inicjatywy EuroPKI służy promowaniu rozwiązań korzystających z kryptografii klucza publicznego w aplikacjach sieciowych. W związku z tym odpowiedzialność urzędu certyfikacyjnego będzie ograniczona do gwarancji podjęcia wszelkich niezbędnych środków do ochrony klucza prywatnego urzędu certyfikacyjnego przed kradzieżą, nadużyciem, utratą i że tożsamość zleceniodawcy będzie należycie zweryfikowana.

Odpowiedzialność urzędu rejestracyjnego

Odpowiedzialność urzędu rejestracyjnego będzie ograniczona do gwarancji wykonania wszelkich niezbędnych kontroli do weryfikacji tożsamości użytkowników końcowych.

Odpowiedzialność finansowa

Użytkownik końcowy akceptuje fakt, że urząd certyfikacyjny nie ponosi odpowiedzialności finansowej za certyfikaty wystawione w ramach niniejszej Polityki Certyfikacji.

Odszkodowanie dla strony ufającej

Bez klauzuli.

Relacje powiernicze

Bez klauzuli.

Procesy administracyjne

Bez klauzuli.

Interpretacja i egzekwowanie aktów prawnych

Prawo nadrzędne

W rozumieniu prawa polskiego, tj. ustawy o podpisie elektronicznym, Dziennik Ustaw 130 z dnia 15.11.2001r., Polskie Centrum Certyfikacji EuroPKI nie jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne.

Rozłączność postanowień, przetrwanie postanowień, połączenie się postanowień, powiadomienia

Bez klauzuli.

Procedury rozstrzygania sporów

Bez klauzuli.

Opłaty

Nie przewiduje się pobierania opłat za świadczenie usług certyfikacyjnych co najmniej do czasu zakończenia projektu NASTEC, tj. do dnia 31.05.2003 roku.

Opłaty za wydanie i odnowienie certyfikatu

Bez klauzuli.

Opłaty za udostępnienie certyfikatu

Bez klauzuli.

Opłaty za unieważnienie i informacje o statusie certyfikatu

Bez klauzuli.

Opłaty za inne usługi takie jak informacje o polityce
Bez klauzuli.

Polityka refundacji
Bez klauzuli.

Publikacja i repozytorium

Publikacja informacji o urzędzie certyfikacyjnym
Następujące informacje dotyczące urzędu certyfikacyjnego muszą być dostępne publicznie:

- polityka certyfikacji oraz kodeks postępowania certyfikacyjnego;
- wszystkie wystawione certyfikaty urzędów certyfikacyjnych;
- certyfikaty tych subskrybentów, którzy zezwolili na publikację certyfikatu;
- lista odwołanych certyfikatów podpisana przez urząd certyfikacyjny.

Częstotliwość publikacji
Jeżeli ulega modyfikacji polityka certyfikacji lub kodeks postępowania certyfikacyjnego, to aktualna wersja tych dokumentów powinna zostać opublikowana równocześnie z terminem ich wejścia w życie. Certyfikaty powinny być publikowane natychmiast po ich wystawieniu i odesłaniu do subskrybenta.

Kontrola dostępu
Nie przewiduje się żadnych niestandardowych metod ochrony dostępu do polityki certyfikacji, kodeksu postępowania certyfikacyjnego oraz list odwołanych certyfikatów. W przypadku ataków sieciowych na repozytorium urząd certyfikacyjny zastrzega sobie prawo do ograniczenia dostępu do repozytorium tylko dla użytkowników poświadczonych przez EuroPKI (poprzez mechanizm SSL z uwierzytelnianiem klienta).

Repozytoria
Informacja wymieniona powyżej jest utrzymywana i udostępniana za pomocą serwisu http:

- Certyfikaty kluczy publicznych są publikowane pod adresem:
  http://www.europki.pl/polish_ca/certs/pl_index.html
- Lista odwołanych certyfikatów jest publikowana pod adresem:
  http://www.europki.pl/polish_ca/crl/pl_index.html
- Polityka certyfikacji jest publikowana pod adresem:
  http://www.europki.pl/polish_ca/cps/pl_index.html
- Kodeks postępowania certyfikacyjnego jest publikowany pod adresem:
  http://www.europki.pl/polish_ca/cps/pl_index.html

Audyt zgodności

Nie przewiduje się żadnych zewnętrznych kontroli usługi i zgodności funkcjonowania z polityką certyfikacji i kodeksem postępowania certyfikacyjnego. Wszelką odpowiedzialność ponosi instytucja świadcząca usługi certyfikacji.

Częstotliwość audytu
Bez klauzuli.

Tożsamość/kwalifikacje audytora
Bez klauzuli.

Związek audytora z audytowaną jednostką
Bez klauzuli.

Zagadnienia obejmowane przez audyt
Bez klauzuli.

Działania podejmowane w celu usunięcia usterek wykrytych podczas audytu
Bez klauzuli.

Informowanie o wynikach audytu
Bez klauzuli.

Poufność

Urzędy certyfikacyjne nie mają prawa przechowywania kluczy prywatnych subskrybentów. Jeżeli urząd generuje parę kluczy dla subskrybenta, to klucz prywatny jest usuwany z wszystkich nośników natychmiast po jego przekazaniu subskrybentowi. Urzędy certyfikacyjne zawsze same generują parę kluczy i przekazują urzędowi nadrzędnemu zlecenie certyfikacji.

Typy informacji traktowane jako poufne
Wszystkie dane subskrybentów, które nie są zawarte w certyfikacie i liście odwołanych certyfikatów wystawionej przez odpowiedni urząd certyfikacyjny są traktowane jako poufne i nie mogą być udostępniane bez wyraźnego upoważnienia subskrybenta.

Typy informacji nie traktowane jako poufne
Informacje zawarte w certyfikatach klucza publicznego i liście odwołanych certyfikatów wystawionej przez odpowiedni urząd certyfikacyjny nie są traktowane jako poufne.

Ujawnienie informacji o odwołaniu/zawieszeniu certyfikatu
Kiedy certyfikat jest odwołany/zawieszony kod przyczyny odwołania/zawieszenia MOŻE być zawarty we wpisie listy odwołanych certyfikatów. Jednak żadne inne szczegóły dotyczące odwołania nie są ujawnione.

Udostępnianie informacji organom administracyjnym i sądowym
Odpowiedni urząd certyfikacyjny nie ujawnia informacji o certyfikacie żadnej osobie trzeciej, z wyjątkiem przypadku wymagania przez organy administracyjne lub sądowe za okazaniem odpowiedniego nakazu.

Udostępnianie w celach naukowych
Bez klauzuli.

Udostępnianie na żądanie właściciela
Urząd certyfikacyjny nie ujawnia informacji o certyfikacie żadnej osobie trzeciej, z wyjątkiem przypadku wymagania przez właściciela z pisemnym wnioskiem.

Inne okoliczności udostępniania informacji
Bez klauzuli.

Prawo do własności intelektualnej

Urząd certyfikacyjny nie może rościć sobie jakichkolwiek praw własności intelektualnej do wydanych certyfikatów.

IDENTYFIKACJA I UWIERZYTELNIANIE

Rejestracja wstępna

Typy nazw

Ceryfikaty urzędu certyfikacyjnego oraz rejestracyjnego muszą mieć niepuste pole zawierające nazwę podmiotu *(subject)*, dla którego zostaje poświadczony klucz publiczny. Pole podmiotu musi zawierać wyróżnioną nazwę zgodną ze standardem X.500. Urząd certyfikacyjny musi również stosować w nazwie alternatywnej podmiotu dodatkowe dane identyfikacyjne: adres e-mail oraz adres typu URL, wskazujący stronę WWW urzędu.

Konieczność nazw znaczących

Nazwa wyróżniona musi w sposób jednoznaczny identyfikować certyfikowany urząd. Zgodnie z polityką EuroPKI ([1]) nazwa ta musi być znacząca, tzn. musi pozwalać zidentyfikować jednostkę w odpowiedniej instytucji.

Zasady interpretacji różnych form nazw

Zawsze, gdy urząd zlecający certyfikacje swego klucza żąda umieszczenia nazwy wyróżnionej skojarzonej z konkretną instytucją, odpowiedni urząd certyfikacyjny lub rejestracyjny musi otrzymać poświadczenie, że dana instytucja wie o tym fakcie.

Unikatowość nazw

Nazwy muszą być unikatowe w drzewie danych katalogowych (X.500/LDAP). Nazwa wyróżniona musi być unikatowa dla każdej jednostki podmiotu certyfikowanego przez Polskie Centrum Certyfikacji EuroPKI.

Procedura rozwiązywania sporów wynikających z reklamacji nazw

Urząd certyfikacyjny ma decydujący głos w spornych sprawach dotyczących nazwy wyróżnionej subskrybenta.

Rozpoznawanie, uwierzytelnianie i rola znaków towarowych

Bez klauzuli.

Metody dowodu posiadania klucza prywatnego

Dopuszcza się dwie sytuacje:

- urząd certyfikacyjny lub użytkownik końcowy zleca certyfikację swego klucza publicznego. Urząd certyfikacyjny lub użytkownik końcowy sam generuje parę kluczy, a następnie przygotowuje zlecenie certyfikacji i podpisuje je. Następnie dostarcza zlecenie certyfikacji oraz wynik działania funkcji skrótu w formie papierowej;
- użytkownik końcowy zgłasza się do urzędu certyfikacyjnego w celu wystawienia mu pary kluczy oraz scertyfikowania klucza publicznego.

W pierwszej sytuacji zakłada się, że subskrybent jest właścicielem odpowiedniego klucza prywatnego. W drugim przypadku urząd certyfikacyjny sam generuje klucz prywatny i przekazuje go zleceniodawcy, co wyklucza podejrzenia w odniesieniu do tego klucza.

Uwierzytelnianie danych instytucji

Certyfikacja odbywa się na podstawie umowy podpisanej przez dwie strony: urząd zlecający certyfikację swego klucza publicznego oraz jego urząd nadrzędny. Urząd rejestrujący weryfikuje tożsamość zleceniodawcy oraz potwierdza jego uprawnienia do występowania w roli określonego urzędu certyfikacyjnego. Weryfikacja tożsamości następuje za pomocą takich danych identyfikujących jak dowód osobisty, paszport, czy inny dokument należący do osoby oficjalnie reprezentującej daną instytucję. Potwierdzenie uprawnień do występowania w roli określonego urzędu jest realizowane na podstawie dostarczonej umowy będącej formą

uprawomocnienia funkcjonowania w określonym środowisku. W uzasadnionych sytuacjach mogą zostać podjęte dodatkowe działania zmierzające do potwierdzenia wiarygodności certyfikowanego urzędu.

Uwierzytelnianie tożsamości użytkownika

Tożsamość osoby ubiegającej się o certyfikację klucza publicznego jest weryfikowana na podstawie dowodu tożsamości (dowód osobisty, paszport, prawo jazdy).

Odnowienie certyfikatu

Ponowne wystawienie certyfikatu jest możliwe wyłącznie na zlecenie, gdy dobiega końca termin ważności poprzedniego certyfikatu związanego z określonym kluczem publicznym. Czynność ponownej certyfikacji nie może zostać zrealizowana, gdy poprzedni certyfikat został odwołany lub uległ już przedawnieniu. Urząd certyfikacyjny lub użytkownik końcowy ubiegający się o ponowną certyfikację musi wysłać przed wygaśnięciem poprzedniego certyfikatu do swojego urzędu nadrzędnego zlecenie certyfikacji (w formacie PKCS#10, zakodowane zgodnie ze standardem PEM lub DER). W tej sytuacji nie są podejmowane procedury zmierzające do identyfikacji i uwiarygodnienia zlecenia. Ponowna certyfikacja jest możliwa wyłącznie w przypadku, gdy nie ulega zmianie wyróżniona nazwa podmiotu. Urząd certyfikacyjny ma prawo odmówić ponownej certyfikacji zlecającemu urzędowi lub użytkownikowi końcowemu.

Odnowienie po unieważnieniu

Nie jest możliwe wystawienie certyfikatu na podstawie klucza publicznego, którego poprzedni certyfikat urząd certyfikacyjny odwołał. Subskrybent musi ubiegać się o certyfikat za pomocą typowych procedur.

Żądanie unieważnienia certyfikatu

Urząd certyfikacyjny musi zidentyfikować osobę przekazującą zlecenie odwołania certyfikatu. Jedną z metod uwierzytelnienia jest poświadczenie przekazywanego komunikatu własnym podpisem (do którego użyto aktualnego i nie odwołanego certyfikatu). Do sprawdzenia wiarygodności zlecenia należy stosować takie same procedury, jakie obowiązują w procesie rejestrowania subskrybenta. Dopuszcza się wprowadzenie w tym celu specjalnych metod gwarantujących bezpieczną komunikację; metody takie muszą zostać zdefiniowane w kodeksie postępowania certyfikacyjnego urzędu, w którym obowiązują.

WYMAGANIA FUNKCJONALNE

Ubieganie się o certyfikat

Subskrybent musi zapoznać się i zaakceptować Politykę Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego i potwierdzić to podpisanym oświadczeniem.

Tożsamość subskrybenta weryfikuje urząd certyfikacyjny lub wspomagający go urząd rejestracyjny. Urząd rejestracyjny może potwierdzić autentyczność zlecenia certyfikacji (na podstawie dodatkowego hasła lub specjalnego skrótu danych; sposób potwierdzenia jest definiowany w dwustronnej umowie między urzędem certyfikacyjnym a zleceniodawcą).

Urząd certyfikacyjny ubiegający się o poświadczenie klucza publicznego sam generuje parę kluczy o rozmiarze minimum 1024 oraz sam dba o bezpieczne przechowywanie klucza

prywatnego, który musi być chroniony za pomocą szyfrowania (np. szyfrowanie oparte na haśle). Do generowania kluczy oraz przechowywania klucza prywatnego mogą być używane techniki sprzętowe lub programowe.

Nadrzędny urząd certyfikacyjny NIGDY NIE GENERUJE pary kluczy dla urzędu podporządkowanego. Nadrzędny urząd certyfikacyjny nie bierze odpowiedzialności za zniszczenie lub uszkodzenie klucza wynikające z jego niepoprawnego wygenerowania lub złego przechowywania.

Niniejsza polityka ustala, że urząd certyfikacyjny lub urząd rejestracyjny, którego klucz publiczny ma zostać poświadczony przez urząd nadrzędny (np. Polskie Centrum Certyfikacji EuroPKI) musi dostarczyć podpisane przez siebie zlecenie certyfikacji w formacie PKSC#10. Zlecenie certyfikacji jest przekazywane do urzędu certyfikacyjnego za pomocą poczty elektronicznej lub poprzez zewnętrzny nośnik danych, np. dyskietkę, CD-ROM. Zlecenie certyfikacji musi zostać przygotowane w formacie DER lub PEM.

Użytkownik końcowy może przekazać zlecenie certyfikacji urzędowi, który ma poświadczyć jego klucz publiczny. Zlecenie certyfikacji jest przygotowywane po samodzielnym wygenerowaniu pary kluczy lub może zlecić urzędowi certyfikacyjnemu generację pary kluczy i następnie certyfikację klucza publicznego.

Wydanie certyfikatu

Urząd certyfikacyjny wystawia certyfikat zgodnie z polityką zdefiniowaną w dokumencie [1]. Termin ważności certyfikatu jest ustalany w umowie, ale nie może przekraczać okresu ważności certyfikatów zdefiniowanego w niniejszej polityce obowiązującym dla Polskiego Centrum Certyfikacji EuroPKI.

W uzasadnionych przypadkach urząd certyfikacyjny ma prawo odmowy realizacji zlecenia certyfikacji.

Cetryfikaty wystawiane przez urzędy certyfikacyjny działające na podstawie niniejszej polityki są certyfikatami zgodnymi ze standardem X.509v3.

Gotowy certyfikat jest dostarczany zleceniodawcy za pomocą poczty elektronicznej lub dowolnego zewnętrznego nośnika danych (dyskietka, CD-ROM), zgodnie z wymaganiami określonymi w umowie. Urząd odbierający certyfikatu otrzymuje również pełny łańcuch certyfikatów, czyli zestaw wszystkich certyfikatów umożliwiających weryfikację (lista w formacie PKCS#7 zakodowana do postaci PEM lub DER).

Urzędy certyfikacyjne mają prawo publikacji każdego wystawionego certyfikatu za pomocą bazy katalogowej LDAP lub zasobów HTTP, o ile urząd zlecający certyfikację swojego klucza lub użytkownik końcowy nie zabroni takiego działania w umowie.

Akceptacja certyfikatu

Bez klauzuli.

Zawieszenie i unieważnienie certyfikatu

Okoliczności unieważnienia certyfikatu

Urząd certyfikacyjny może odwołać certyfikat w następujących przypadkach:

- uległy zmianie dane dotyczące subskrybenta;
- została naruszona wiarygodność klucza prywatnego subskrybenta lub istnieje takie podejrzenie;
- istnieje podejrzenie, że dane zawarte w certyfikacie nie są prawdziwe;
- wiadomo, że subskrybent naruszył swoje zobowiązania.

Kto może żądać unieważnienia certyfikatu

Z wnioskiem o odwołanie certyfikatu może wystąpić jego właściciel, jednostka dostarczająca dowód naruszenia wiarygodności klucza, urząd rejestracyjny lub urząd certyfikacyjny.

Procedura unieważniania certyfikatu

Jednostka żądająca odwołania musi zostać uwierzytelniona przez urząd certyfikacyjny. Zgodnie z dokumentem [1] urząd certyfikacyjny akceptuje zlecenie odwołania certyfikatu, które jest podpisane cyfrowo za pomocą poprawnego certyfikatu (tzn. takiego, który nie jest odwołany ani przedawniony). Alternatywną metodą jest dostarczenie dowodu naruszenia wiarygodności klucza podczas osobistej wizyty w urzędzie certyfikacyjnym, pełnącym funkcję urzędu rejestracyjnego.

Urząd certyfikacyjny ma prawo w uzasadnionych przypadkach sam podjąć decyzję o odwołaniu certyfikatu.

Okres realizacji zlecenia unieważnienia certyfikatu

Zlecenie odwołania certyfikatu musi zostać zrealizowane w ciągu 24 godzin od jego przyjęcia przed odpowiedni urząd.

Okoliczności zawieszania certyfikatu

Urząd certyfikacyjny może na życzenie swojego subskrybenta czasowo zawiesić jego certyfikat. Zawieszony certyfikat może zostać wznowiony w dowolnym czasie. Specjalne repozytoria utrzymywane przez urząd certyfikacyjny gromadzą informacje o zawieszonych certyfikatach.

Kto może żądać zawieszenia certyfikatu

Zawieszenia certyfikatu może zażądać jego posiadacz.

Procedura zawieszania certyfikatu

Wnioskodawca zawieszenia certyfikatu musi stawić się w urzędzie certyfikacyjnym badź rejestracyjnym i okazać swój dokument tożsamości.

Ograniczenia okresu zawieszenia certyfikatu

Bez klauzuli.

Częstotliwość publikowania list unieważnionych certyfikatów (CRL)

Urząd certyfikacyjny co najmniej raz w miesiącu publikuje listę unieważnionych certyfikatów. Lista taka jest aktualizowana za każdym razem, gdy ulega odwołaniu certyfikat wystawiony przez ten urząd. Lista odwołanych certyfikatów jest podpisywana cyfrowo przez wystawiający ją urząd certyfikacyjny. Każdy certyfikat wystawiany urząd certyfikacyjny działający zgodnie z niniejszą polityką zawiera rozszerzenie *CRL Distribution Points* zawierające adresy typu URL, pod którymi są dostępne listy unieważnionych certyfikatów.

Wymagania dotyczące sprawdzania list unieważnionych certyfikatów

Strona ufająca musi sprawdzić ważność certyfikatu w oparciu o aktualną listę unieważnionych certyfikatów opublikowaną przez odpowiedni urząd certyfikacyjny.

Dostępność sprawdzania unieważnienia/statusu on-line

Polskie Centrum Certyfikacji EuroPKI nie udostępnia sprawdzania unieważnienia/statusu

on-line.

Wymagania dotyczące sprawdzania unieważnienia on-line
Bez klauzuli.

Inne dostępne formy ogłaszania unieważnień
Bez klauzuli.

Wymagania dotyczące sprawdzania dla innych form ogłaszania unieważnień
Bez klauzuli.

Wymagania specjalne dotyczące kompromitacji klucza
Bez klauzuli.

Procedury audytu bezpieczeństwa

Typy rejestrowanych zdarzeń
Bez klauzuli.

Częstotliwość przetwarzania zapisów
Bez klauzuli.

Okres przechowywania zapisów dla audytu
Bez klauzuli.

Ochrona zapisów dla audytu
Bez klauzuli.

Procedury tworzenia kopii zapisów dla audytu
Bez klauzuli.

System odbioru audytu
Bez klauzuli.

Powiadamianie podmiotów powodujących zdarzenia
Bez klauzuli.

Oszacowanie podatności na zagrożenia
Bez klauzuli.

Archiwizacja danych

Wszystkie wystawione certyfikaty oraz listy odwołanych certyfikatów są przechowywane w lokalnej bazie danych urzędu certyfikacyjnego. To samo dotyczy wszystkich zleceń certyfikacji, dla których wystawiono certyfikaty, komunikatów urzędów rejestracyjnych związanych z certyfikacją oraz wszystkich podpisanych umów między urzędami.

Rodzaje archiwizowanych danych
Urząd rejestracyjny musi archiwizować wszystkie informacji otrzymane od subskrybenta w procesie rejestracji oraz wszystkie komunikaty wymieniane z urzędem certyfikacji dotyczące subskrybentów.

Okres przechowywania archiwum
Minimalny okres archiwizacji wynosi pięć lat.

Ochrona archiwum
Bez klauzuli.

Procedury tworzenia kopii archiwum
Bez klauzuli.

Wymagania dotyczące znakowania danych znacznikiem czasu
Bez klauzuli.

System zbierania archiwów
Bez klauzuli.

Procedury dostępu i weryfikacji zarchiwizowanych informacji
Bez klauzuli.

Zmiana kluczy

Bez klauzuli.

Odtworzenie po kompromitacji i katastrofie

Jeżeli stwierdzono lub podejrzewa się, że naruszono wiarygodność klucza prywatnego urzędu certyfikacyjnego, to urząd korzystający z tego klucza ma obowiązek:

- poinformować swoich subskrybentów, pośrednie urzędy certyfikacyjne oraz strony korzystające z certyfikatów;
- zaprzestać korzystania z niewiarygodnego klucza prywatnego podczas świadczenie usługi certyfikacji oraz wystawiania list odwołanych certyfikatów;
- zażądać odwołania certyfikatu w nadrzędnym urzędzie certyfikacyjnym.

Jeśli stwierdzono naruszenie wiarygodności klucza prywatnego urzędu rejestracyjnego lub istnieje podejrzenie naruszenia jego wiarygodności, to urząd rejestracyjny musi:

- poinformować wszystkie zainteresowane strony;
- zażądać odwołania certyfikatu w nadrzędnym urzędzie certyfikacyjnym.

Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych
Bez klauzuli.

Unieważnienie klucza publicznego
Bez klauzuli.

Kompromitacja klucza
Bez klauzuli.

Zabezpieczenie środków po katastrofie naturalnej bądź innego typu
Bez klauzuli.

Zakończenie działalności urzędu certyfikacyjnego

Jeśli urząd certyfikacyjny decyduje się zakończyć świadczenie usług certyfikacji, to powinien poinformować o tym wszystkie zainteresowane strony i zakończyć dystrybucję certyfikatów i list odwołanych certyfikatów. Wszystkie wystawione certyfikaty oraz certyfikaty urzędu kończącego działalność muszą zostać odwołane.

Urząd certyfikacyjny, którego certyfikat został odwołany przez Polskie Centrum Certyfikacji EuroPKI powinien:

- poinformować swoich subskrybentów oraz scertyfikowane pośrednio urzędy certyfikacyjne;

- zakończyć świadczenie usługi certyfikacji i wystawiania list odwołanych certyfikatów za pomocą wiarygodnego klucza prywatnego.

KONTROLA ZABEZPIECZEŃ FIZYCZNYCH, PROCEDURALNYCH ORAZ PERSONELU

Kontrola zabezpieczeń fizycznych

Urząd certyfikacyjny musi używać dedykowanej stacji roboczej. Musi być ona zabezpieczona fizycznie.

Lokalizacja i konstrukcja siedziby

Bez klauzuli.

Dostęp fizyczny

Stacje robocze urzędów certyfikacyjnych muszą być umieszczone w pomieszczeniach zabezpieczonych fizycznie. Dostęp do nich mogą mieć wyłącznie osoby posiadające zatwierdzone uprawnienia do wykonywania zadań operatora urzędu. To samo odnosi się do zapasowych stacji roboczych oraz zdeponowanych nośników danych związanych z procesem certyfikacji.

Zasilanie i klimatyzacja

Bez klauzuli.

Zagrożenie zalaniem

Bez klauzuli.

Ochrona przeciwpożarowa

Bez klauzuli.

Nośniki informacji

Bez klauzuli.

Niszczenie informacji

Bez klauzuli.

Kopia bezpieczeństwa poza siedzibą

Bez klauzuli.

Kontrola zabezpieczeń proceduralnych

Zaufane role

Operatorami urzędów certyfikacyjnych są osoby posiadające uprawnienia do wystawiania certyfikatów oraz list odwołanych certyfikatów. Osoby występujące jako urząd rejestracyjny muszą zostać zatwierdzone jako jednostki realizujące proces uwierzytelnienia subskrybenta.

Liczba osób wymaganych do zadania

Każdy urząd certyfikacyjny dysponuje zawsze jednym operatorem gotowym do wykonania bieżących zadań. Dwie do trzech osób są uprawnione i przygotowane do wykonywania obowiązków operatora urzędu cetyfikacyjnego.

Identyfikacja i uwierzytelnianie ról

Bez klauzuli.

Kontrola personelu

Wymagania dotyczące pochodzenia, kwalifikacji, doświadczenia i odprawy

Urząd certyfikacyjny ponosi odpowiedzialność za właściwe przygotowanie i kompetencje swoich operatorów, a także gwarantuje operatorom dostęp do wszystkich narzędzi potrzebnych w procesie certyfikacji. Urząd certyfikacyjny zapewnia poufność i bezpieczeństwo swoich urzędów rejestracyjnych.

Postępowanie sprawdzające

Bez klauzuli.

Wymagania dotyczące szkoleń

Bez klauzuli.

Częstotliwość powtarzania szkoleń i ich wymagania

Bez klauzuli.

Częstotliwość rotacji stanowisk i ich kolejność

Bez klauzuli.

Sankcje z tytułu nieuprawnionych działań

Operatorzy urzędów certyfikacyjnych i rejestracyjnych, którzy nadużyli swoich uprawnień bezzwłocznie tracą swoją funkcję.

Wymagania dotyczące personelu kontraktowego

Bez klauzuli.

Dokumentacja przekazana personelowi

Bez klauzuli.

KONTROLA BEZPIECZEŃSTWA TECHNICZNEGO

Generacja i instalacja pary kluczy

Generacja pary kluczy

Klucze są generowane za pomocą oprogramowania lub sprzętu. To samo oprogramowanie, które jest używane do wystawiania certyfikatów można stosować do generacji kluczy.

Dostarczanie klucza prywatnego subskrybentowi

Jeśli subskrybent zleca urzędowi wygenerowanie pary kluczy, a następnie certyfikację klucza publicznego, to wygenerowana para kluczy zostaje zaszyfrowana lub umieszczona na karcie typu *smardcard* i w takiej postaci przekazana do subskrybenta. Subskrybent odbiera w urzędzie rejestracyjnym (lub certyfikacyjnym, jeżeli nie korzysta się z urzędów rejestracyjnych) hasło użyte w algorytmie szyfrowania lub identyfikator zastosowany w karcie (PIN). Dane te mogą również zostać przekazane za pomocą bezpiecznej komunikacji sieciowej.

Dostarczanie klucza publicznego do wydawcy certyfikatu

Subskrybenci, którzy sami wygenerowali parę kluczy i przygotowali zlecenie certyfikacji przekazują to zlecenie do urzędu rejestracyjnego (bądź urzędu certyfikacyjnego pełniącego tę funkcję). Urząd rejestracyjny podpisuje zlecenie i przekazuje je urzędowi certyfikacyjnemu.

Dostarczanie użytkownikom klucza publicznego urzędu certyfikacyjnego
Wyszukanie w odpowiednim repozytorium potrzebnych kluczy urzędów certyfikacyjnych i ich załadowanie jest zadaniem użytkownika. Klucz publiczny Root CA powinien być dostępny poprzez środki, którym mogą ufać użytkownicy, zabezpieczony w podpisanym przez siebie certyfikacie.

Długości klucza
Klucz prywatny użytkownika końcowego musi mieć długość co najmniej 1024 bitów. Klucz prywatny urzędu certyfikacyjnego musi mieć długość co najmniej 2048 bitów. Urząd certyfikacyjny odmawia certyfikacji klucza o mniejszym rozmiarze niż obowiązujący.

Generowanie parametrów klucza publicznego
Bez klauzuli.

Sprawdzanie jakości parametrów
Bez klauzuli.

Sprzętowe lub programowe generowanie kluczy
Klucze są generowane przez oprogramowanie.

Cele zastosowania kluczy (wg pól zastosowania klucza X.509 v3)
Bez klauzuli.

Ochrona klucza prywatnego

Standard modułu kryptograficznego
Klucze prywatne powinny być przechowywane w postaci zaszyfrowanej na płycie CD-ROM, dyskietce lub na nośniku typu *smartcard*. Hasło chroniące klucz powinno mieć właściwą jakość.

Kontrola klucza prywatnego przez wiele osób
Klucz prywatny indywidualny nie jest pod kontrolą wielu osób. Klucze prywatne należące do urzędu certyfikacyjnego znajdują się pod taką kontrolą.

Depozyt klucza prywatnego
Bez klauzuli.

Kopie zapasowe klucza prywatnego
Aktualnie nie przewiduje się przechowywania kopii zapasowych kluczy prywatnych subskrybentów. Kopia zapasowa klucza prywatnego Polskiego Centrum Certyfikacji EuroPKI jest przechowywana na stacji roboczej urzędu certyfikacyjnego oraz dodatkowo będzie zdeponowana w Kancelarii Tajnej Politechniki Wrocławskiej.

Archiwizacja klucza prywatnego
Klucze prywatne nie są archiwizowane.

Wprowadzanie klucza prywatnego do modułu kryptograficznego
Bez klauzuli.

Metoda aktywacji klucza prywatnego
Aktywacja klucza prywatnego wymaga podania przez właściciela odpowiedniego hasła.

Metoda dezaktywacji klucza prywatnego
Bez klauzuli.

Metoda niszczenia klucza prywatnego
Bez klauzuli.

Inne aspekty zarządzania kluczami

Archiwizacja kluczy publicznych
Wszystkie klucze publiczne, na podstawie których dokonano certyfikacji są archiwizowane przez urząd certyfikacyjny.

Okresy stosowania kluczy publicznych i prywatnych
Bez klauzuli.

Dane aktywacyjne

Generacja i instalacja danych aktywacyjnych
Hasła używane do ochrony danych przesyłanych w procesie certyfikacji oraz chroniące wygenerowane klucze powinny być dobierane według ogólnie znanych zaleceń dotyczących haseł.

Ochrona danych aktywacyjnych
Hasła muszą być tak przechowywane, by nie trafiły do osób nieupoważnionych.

Inne aspekty dotyczące danych aktywacyjnych
Bez klauzuli.

Kontrola bezpieczeństwa komputerowego

Urząd certyfikacyjny musi używać dedykowanej stacji roboczej.

Specyficzne wymagania techniczne dotyczące bezpieczeństwa komputerowego
Bez klauzuli.

Ocena bepiczeństwa komputerowego
Bez klauzuli.

Cykl kontroli technicznej

Kontrola rozwoju systemu
Bez klauzuli.

Kontrola zarządzania bezpieczeństwem
Bez klauzuli.

Ocena bezpieczeństwa cyklu
Bez klauzuli.

Kontrola bezpieczeństwa sieci

Stacja komputerowa, na której są realizowane zadania urzędu certyfikacyjnego nie może mieć połączeń sieciowych, jeśli na jej dysku jest przechowywany klucz prywatny tego urzędu. Wymiana danych między tą stacją a resztą środowiska biorącego udział w procesie ceryfikacji musi odbywać się za pomocą zewnętrznych nośników danych (dyski, dyskietki, ZIP-drive).

Kontrola inżynierii modułu kryptograficznego

Bez klauzuli.

PROFILE CERTYFIKATU I LISTY UNIEWAŻNIONYCH CERTYFIKATÓW

Profil certyfikatu

Bez klauzuli.

Numer wersji
Bez klauzuli.

Rozszerzenia certyfikatu
Bez klauzuli.

Identyfikatory algorytmu
Bez klauzuli.

Formy nazw
Bez klauzuli.

Ograniczenia nazw
Bez klauzuli.

Identyfikator polityki certyfikacji
Bez klauzuli.

Stosowanie rozszerzenia ograniczeń polityki
Bez klauzuli.

Składnia i semantyka kwalifikatorów polityki
Bez klauzuli.

Semantyka przetwarzania dla rozszerzenia krytycznego polityki certyfikacji
Bez klauzuli.

Profil listy unieważnionych certyfikatów

Numer wersji
Bez klauzuli.

Rozszerzenia CRL i wpisu CRL
Bez klauzuli.

ADMINISTROWANIE SPECYFIKACJĄ

Procedura zmiany specyfikacji

Dopuszcza się realizację zmian typu edytorskiego w niniejszej polityce. O aktualizacjach dotyczących aspektów technicznych lub proceduralnych należy powiadamiać z uprzedzeniem. Podporządkowane urzędy certyfikacyjne mają obowiązek dostosowania swojej polityki do bieżącej wersji niniejszego dokumentu.

Polityki publikacji i powiadamiania

Niniejsza polityka będzie dostępna poprzez WWW.

Procedura zatwierdzania polityki certyfikacji

Bez klauzuli.

REFERENCJE

[1] EuroPKI Certificate Policy, Version 1.1. (Draft 4), October 2000,
OID: 1.3.6.1.4.1.5255.1.1.1.

Załącznik 2 Deklaracji

DEKLARACJA

Ja, niżej podpisany/a, _____ ,
(imię i nazwisko)

reprezentujący/a _____ ,
(nazwa instytucji)

niniejszą deklaracją wnoszę o uruchomienie urzędu certyfikacji w ramach hierarchii EuroPKI.

Zobowiązuję się:

- stosować do zasad polityki certyfikacji EuroPKI;
- napisać własny Kodeks Postępowania Certyfikacyjnego i uzyskać akceptację Polskiego Centrum Certyfikacji EuroPKI;
- wydawać certyfikaty dla każdego zleceniodawcy, wyłącznie wewnątrz grup wyszczególnionych w Kodeksie Postępowania Certyfikacyjnego;
- informować nadrzędny urząd certyfikacji o wszelkich zmianach.

Deleguję:

_____
(imię i nazwisko osoby delegowanej)

telefon: _____

e-mail: _____

jako osobę odpowiedzialną za nadzór techniczny urzędu.

Miejscowość Data

Imię i nazwisko

Podpis

Załącznik 3 Zlecenie certyfikacji

ZLECENIE CERTYFIKACJI

Ja, niżej podpisany/a,

……..... ,
(imię i nazwisko)

jako osoba odpowiedzialna za sprawy techniczne Urzędu Certyfikacji

..... ,
(nazwa Urzędu Certyfikacji)

pełniący/a obowiązki

..... ,
(nazwa funkcji)

składam zlecenie wydania certyfikatu klucza publicznego dla wyżej wymienionego urzędu certyfikacji.

W celu autentyczności niniejszego zlecenia, przedstawiam skrót wyliczony z pliku zawierającego zlecenie certyfikacji za pomocą algorytmu (wskazać SHA1 lub MD5):

.....

o wartości (szesnastkowo):

.....

.....

Proszę ustawić datę wygaśnięcia ważności certyfikatu na:

.....

Miejscowość **Data**

Imię i nazwisko

Podpis