Leiðbeiningar fyrir uppsetningu rafrænna skilríkja í Apache

Inngangur - Yfirlit

Fullgildu rafrænu skilríkin á örgjörvakortum eru gefin út af milliskilríkinu Fullgilt audkenni sem er aftur gefið út af rótinni Íslandsrót.

Til að nýta rafræn skilríki þarf ekki að gera annað en stilla vefmiðlara þannig að hann noti Íslandsrót og millirskilríkið Fullgilt audkenni til að votta rafrænu skilríkin.

Hægt er að hugsa sér framkvæmdina sem 3 skref:

1. Gerðu vefmiðlarann þinn SSL-hæfan með vefskilríki.
   (Slóðin að innskráningarsíðunni verður að vera https)
2. Bættu Íslandsrót og Fullgilt audkenni við skilgreiningar í vefmiðlaranum þínum.
   Hér getur þú sótt þessi tvö skilríki:
   Íslandsrót http://www.audkenni.is/rafraenskilriki/kedjur/Islandsrot.zip
   Fullgilt audkenni http://www.audkenni.is/rafraenskilriki/kedjur/Fullgilt_audkenni.zip
3. Skilgreindu svæði á miðlaranum þar sem krefjast á rafræns skilríkis.

SSL aðgangsstýring í Apache (demo)

Leiðbeiningar fyrir CentOS 3 miðlara sem keyrir Apache 2.0.46 með OpenSSL 0.9.7a.
VirtualHost www.len.is.

Aðgangsstýringin felst í grunnin í því að Íslandsrót og Fullgilt audkenni er treyst (bætt í skrána sem SSLCACertificateFile bendir á)

SSLCACertificateFile /etc/httpd/conf/ssldemo/v2-cacertfile.crt

-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIBATANBgkqhkiG9w0BAQUFADB0MQswCQYDVQQGEwJJUzET
MBEGA1UEBRMKNTUwMTY5MjgyOTEaMBgGA1UEChMRRmphcm1hbGFyYWR1bmV5dGkx
FjAUBgNVBAsTDVJvdGFyc2tpbHJpa2kxHDAaBgNVBAMTE0lzbGFuZHNyb3QgLSBw
cm9mdW4wHhcNMDcwMzI2MTkwMjAxWhcNMzIwMzI2MTk1NjQ2WjB0MQswCQYDVQQG
EwJJUzETMBEGA1UEBRMKNTUwMTY5MjgyOTEaMBgGA1UEChMRRmphcm1hbGFyYWR1
bmV5dGkxFjAUBgNVBAsTDVJvdGFyc2tpbHJpa2kxHDAaBgNVBAMTE0lzbGFuZHNy
b3QgLSBwcm9mdW4wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDH9yup
X3pMxVFbAuH+asPJ4JYO0hcd2293PMRZln4i9wR/KrQpC8Lvf0Mc1Un/SDx+jpED
BFhpz1XPbSw9wvT0S7cz0vPBPpOZAHi87nfat5Evgd9I+PWMupiTh2ef2gvosOla
som783KSW77v0go9ZEVBOQzda2YSfDyY2K0eo4tunzkGsIQyOFGKhqvlqaWZoxFL
7R0dKE51wn1Doi6HdAIJCky/ICjfwz8bf4yecuw4KaKq3IZQWP2sp59yxOZS/8fp
/p/80C4Er+fniH444cuYk8o5mJFZWKImFmgt573SQsPsQNNh3JjQ4q6dOCv2lCAc
NfMeZqpZ0uO/3gHtZ8Y7xhN5tbxesShjZcjqt5aBPcT+TFeCy/mBoRJqzrZvDt2c
c2R6eYMb5TlpIASuW7LzAe3F29v+q4sUGBPfB7WXEhY3hShL9+oDl5LjodFRohxc
K3qY5jwc3JB9n+X1svj28DhLkaZhiTYNpQc4euKGtNBHHIZ2+QaVTJV0khdQCvg0
CPKxtgwkq3WQRNNEecMCim78Fwi6gv+5QRawDIOqeSw8Uos4MzPujTbBdfJiJmEg
LILStNV9dysz/hKZ4f15hx3tJBXgDkgB2o2K7exYP7yPRyie8BHHMgCk+ml97t9h
WQTyhBCD1rObKeX49qvCZ8gxmWoEr95I5ZoDaQIDAQABo4GwMIGtMBIGA1UdEwEB
/wQIMAYBAf8CAQIwaAYDVR0gBGEwXzBdBghggmABAYdnATBRMCUGCCsGAQUFBwIC
MBkaF0NlcnRpZmljYXRlIFJvb3QgUG9saWN5MCgGCCsGAQUFBwIBFhxodHRwczov
L3d3dy5pc2xhbmRzcm90LmlzL2NwMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQU

8/mWCb/r+kAGP407otRraX6LzZwwDQYJKoZIhvcNAQEFBQADggIBAGBP9fuMfSaX
TsvdaCLi7YpUW+kIdXvCUDAmNnHab3WKO0HtCqOPMeUIktcO3Y1sVCSl+fbMVWl2
MRcCmz4OOC4GXO/BsnKCnAjYKoByGh4IEL92iLBPADyJbU72CeGtuYMyOkXLSsTS
daLwHCTLbCk6TpbIQRG1hDhB1/RnEBn4MgubIKPr2bOaiS9kZQPdSFK4LjJOF61R
NAtFV7YvjXotXDaAOQq8/XBzmhF17F9mSV+v9NTX8UdQe3BbK51FdIigcBOPcZma
NRcCrcmuOCJzx1c+Z7LMo/TXfUZGAyDsAui7AsnMGNP5OlQ7LG1Jc23oIGfR/xTM
fr/5Q2zuACzACcCEcePhG2TeAmeKh37tKrINq5MkagVsyAzxIt+tZHW6YmOJc8e5
Ixhl8p6wFOAbkLa6YXdkXfy1YiMeIvFUt+X3cpWtoqiE8nSuohCmy7FbqczPaRvk
d5HNRhbZQpxEhxoS98dMd/j/RF1Vj1RIHdLsNxFL6Zh68qdxb/w1XI4GpGITtAIS
Tt/r/wi2VBdBqiSNjtGq2UbVFB4ySaANqKX+NP8XPZMaWn0dcWpE9bMtXQeH30ce
kNeuNMm3ZLdOHlFTITo3gvd5kiDtHXFYAMNDI2QNgfpCfYMKD3qaedFUiRGgqrhN
RO/QQmCMUMp3tYEjvIdk0mPQ0BjGJRAB
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBaTANBgkqhkiG9w0BAQUFADB0MQswCQYDVQQGEwJJUzET
MBEGA1UEBRMKNTUwMTY5MjgyOTEaMBgGA1UEChMRRmphcm1hbGFyYWR1bmV5dGkx
FjAUBgNVBAsTDVJvdGFyc2tpbHJpa2kxHDAaBgNVBAMTE0lzbGFuZHNyb3QgLSBw
cm9mdW4wHhcNMDcwMzI2MjMwMjA1WhcNMTcwMzI2MjMwMTUyWjCBgTELMAkGA1UE
BhMCSVMxEzARBgNVBAUTCjUyMTAwMDI3OTAxFTATBgNVBAoTDEF1ZGtlbm5pIGhm
LjElMCMGA1UECxMcVXRnZWZhbmRpIGF1ZGtlbm5pc3NraWxyaWtqYTEfMB0GA1UE
AxMWVHJhdXN0IEF1ZGtlbm5pLXByb2Z1bjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMRq/sKJRm2qUyCMSxjKAWTDkL8l87iON8Gft0RmOvMuyZvpt5XS
Jz+ROzPfy/HlPn81ytSVFGNHkLP2lAd4Yx1bGg7mabvSHEmzd635SKnulCQsOAHW
wntNKMbOnOETr90s4EYUcLE1WEEPmSwQwGHs5o8FKcqbQk3XtSqbM7CVBqrFtH0U
paqyefaZj9PbWY7lz7yvxO0C4TR3V79FPsAYl0Lg629f8GCW8Vi25D7A3V684mbV
2ocRk1keKii1nQbKvtlUZ5V5/4xPBRK8GPnTKfam/ND8YjLT/8N4Gzl6LpEf8w1h
3KiK4r6IWo5YhmvrSuENjRJu057E9acPpZkCAwEAAaOCATUwggExMA8GA1UdEwEB
/wQFMAMBAf8wgYAGA1UdIAR5MHcwdQYIYIJgAgGHGZwIwaTAtBggrBgEFBQcCAjAh
Gh9JbnRlcm1lZGlhdGUgQ2VydGlmaWNhdGUgUG9saWN5MDgGCCsGAQUFBwIBFixo
dHRwczovL2Nwcy5hdWRrZW5uaS5pcy90cmF1c3RhdWRrZW5uaXByb2Z1bjAOBgNV
HQ8BAf8EBAMCAQYwHwYDVR0jBBgwFoAU8/mWCb/r+kAGP407otRraX6LzZwwSwYD
VR0fBEQwQjBAoD6gPIY6aHR0cHM6Ly9jcmwuaXNsYW5kc3JvdC5pcy9pc2xhbmRz
cm90L2NybF9wcm9mdW4vbGF0ZXN0LmNybDAdBgNVHQ4EFgQUHnS4aCblVTdbZ66V
8pqCL3/8rHgwDQYJKoZIhvcNAQEFBQADggIBAE+8V7HyYMFet8270TNMkD9jqkoG
D4CJjivek5nEG8bwaWnPiEFwsyfCU1AETNRGSm57Lz5j8RKXyXX9RzId3IT7dRF+
PyrIkeuLXl3VP6tewdzz0WQ00RDrvrGH9+1XTqV4Y0LxbSUjXQYsPzjs8oM74QWq
FEx2qId+UhCYIUMF2zWWuLyqpuGl5+PnMJK4BILUMjxd0xenpKWMrFLmZnT0h6HQ
O2bBMokm/6dfcp/kY0GVgTwBcJblXU1RGtkaOL3NV0V9wz++w+Udc1QW8nXa+lW1
fUmnbKrwNGyDFaLxDteaKbYcpGosa3F/N4eSJv1dyGHVCh2S5wUfLSfS9XSbBFjW
a4owNItm8zD4IP61kZoIf0Vc7fdP/FQz7qx0qgtfLD9Xj6jB1VwtPH1GsxdM/nkO
lkXvvU07O53yJtXHxRqLO9m0UBQHYD/E0KzVnxxiFR2sNT77SqhgZO4V80Dsltfr
CWm0VKvS0tGiX4Gatp2nZgUsBf+mLBGfhPw1z3mdEmL3G9Ef5fnjFx09+YV5CeS2
zhTzcQYgIBpGDzu9T6fTcvXC1evp+CId0yus7Y4T0AFJMUNNBUgji9MdBRMMkg8x
MjYB1zhslJEWydD9Hp0V9rIU7Nely1mCZxBLr72taHsWzrPA8x4hYSeV+ve+XAZe
ej3JVu8JWm55dO+E
-----END CERTIFICATE-----

v2-cacertfile.crt er textaskrá sem inniheldur bæði skilríkin á Base64 (PEM) formi.

Ofan á þetta er svo filter á skilríkin sem segir til um hver útgefandinn má vera:

```
SSLRequire %{SSL_CLIENT_I_DN_CN} eq "Fullgilt audkenni"
```

Þannig er eingöngu millirót/útgefanda með CN “ Fullgilt audkenni ” gefinn aðgangur. Hægt er að skrifa flóknari filtera, þrengja skilyrðin, leyfa aðgang frá fleiri en einum útgefanda, ákvarða aðgang miðað við tíma dags o.m.fl.

PHP aðgangur að skilríkjum

PHP kóði hefur aðgang að SSL upplýsingabreytum sem hægt er að vinna hluti eins og kennitölu o.fl. úr skilríkjunum.

```
SSLOptions +StdEnvVars +CompatEnvVars
```

Hjálplegar vefsíður

Apache SSL stillingar:
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html
SSLReqire filterinn:
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslrequire
OpenSSL villukóðar (undir DIAGNOSTICS):
http://www.openssl.org/docs/apps/verify.html
Grunnuppsetning á SSL Client Authentication í Apache:
http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html#accesscontrol

Apache VirtualHost config

Dæmi um Apache VirtualHost config fyrir SSL aðgangsstýrðan vef.

```
# Redirectum http traffík yfir á https:
<VirtualHost www.len.is:80>
ServerName www.len.is
Redirect / https://www.len.is/
</VirtualHost>
# https vefur:
<VirtualHost www.len.is:443>
DocumentRoot /var/www/virtual/www.len.is/html
ServerName www.len.is
ServerAdmin iar@skyrr.is
# Access og error loggar:
CustomLog /var/log/httpd/www.len.is443-access_log combined
ErrorLog /var/log/httpd/www.len.is443-error_log
# SSL stillingar og virkja SSL:
SSLCipherSuite HIGH:MEDIUM
SSLProtocol all -SSLv2
SSLEngine on
# SSL skilriki og lykill vefmiðlara:
SSLCertificateFile /etc/httpd/conf/ssldemo/v-www.len.is.crt
SSLCertificateKeyFile /etc/httpd/conf/ssldemo/v-www.len.is.key
# CA certificate og chain files:
SSLCACertificateFile /etc/httpd/conf/ssldemo/v2-cacertfile.crt
RemoveHandler .css
<Directory "/var/www/virtual/www.len.is/html">
Options Indexes FollowSymLinks MultiViews Includes
AllowOverride All
Order allow,deny
Allow from all
```

```
</Directory>
<Directory "/var/www/virtual/www.len.is/html/Passneeded">
AuthType Basic
AuthName "Username and Password Required"
AuthUserFile /etc/httpd/conf/ssldemo/v-htpasswd
Require valid-user
</Directory>
# Þarf " Fullgilt audkenni " til að komast inn:
<Directory "/var/www/virtual/www.len.is/html/Certneeded">
SSLOptions +StdEnvVars +CompatEnvVars
SSLVerifyClient require
SSLVerifyDepth 2
SSLRequire %{SSL_CLIENT_I_DN_CN} eq "Fullgilt audkenni"
</Directory>
# Þarf eitthvert SSL skilríki (útgefið af CA) til að komast inn
<Directory "/var/www/virtual/www.len.is/html/CertneededAny">
SSLOptions +StdEnvVars +CompatEnvVars
SSLVerifyClient require
SSLVerifyDepth 2
</Directory>
</VirtualHost>
```