Kliens authentikálás és Form Signing

Kliens authentikálás és Form Signing technikai útmutató (Apache webszerver környezetben)

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

1. Tartalomjegyzék

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

2. Bevezető

E tájékoztató célja, hogy bemutassa, milyen beállítások szükségesek a kliens authentikálás használatához Apache webszerveren.

EZEN ÚTMUTATÓ A KLIENS AUTHENTIKÁCIÓ BEÁLLÍTÁSÁT CÉLOZZA MEG ÉS NEM TAGLALJA A WEBSZERVER TANÚSÍTVÁNYÁNAK BEÁLLÍTÁSÁT. AZT A VONATKOZÓ DOKUMENTÁCIÓ TARTALMAZZA,

Amennyiben bármilyen kérdés vagy probléma merül fel, Ügyfélszolgálatunk a (40) 22-55-22 telefonszámon, az info@netlock.hu e-mail címen vagy személyesen a 1101 Budapest, Expo tér 5-7. szám alatt, munkanapokon 9 és 17 óra között készséggel áll rendelkezésére.

3. Minimális rendszerkövetelmények

A TLS szabványban található protokoll szintű hiba miatt a tanúsítványos authentikáció biztonsági problémát okozhat, így a webszerver esetén előírt minimum követelmény:

- Apache httpd 2.2.15 vagy későbbi verzió, OpenSSL 0.9.8m vagy későbbi verzió
- SSL tanúsítvány a szerverhez (ezt cégünk is tudja biztosítani. Igény esetén vegye fel a kapcsolatot Vevőszolgálatunkkal).
- legalább 1 kliens authentikációs tanúsítvány (ezt cégünk is tudja biztosítani. Igény esetén vegye fel a kapcsolatot Vevőszolgálatunkkal.

4. Tanúsítványos authentikálás előnyei

A tanúsítvánnyal történő authentikálás előnyei:

- a felhasználó csak eszköz és tudás birtokában tud belépni a weboldalra, azaz multifaktoros az authentikáció (chipkártya és pin kód)
- a belépéshez szükséges kliens authentikációs tanúsítvány legfelsőbb szintű hitelesítés-szolgáltató által van aláírva (NetLock Kft.), tehát kliens oldali környezetbe hibaüzenetek nélkül applikálható

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

5. Előzetes követelmény – A gyökértanúsítványok beszerzése

Ahhoz, hogy a kliens authentikáció működjön, szükséges a gyökértanúsítványok és köztes tanúsítványok szerver számára elfogadható módon történő telepítése.

Az elfogadni kívánt tanúsítványok kiadója alapján a következő tanúsítványok letöltése szükséges. Mivel egyes böngészők ezt automatikusan megnyitják, a tanúsítvány letöltéséhez célszerű Internet Explorer-t használni.

Az egyes kiadók elérése a következő alfejezetben olvasható.

5.1. SHA 256 kiadók

Az SHA256 algoritmusú kiadók a következő URL-eken érhetők el.

Legfelső szintű kiadó:

Arany	(SHA256)	www.netlock.hu/index.cgi?ca=gold

Köztes szintű kiadó, ha a kliensek csak authentikációs tanúsítványtípust használnak:

Közjegyzői	(SHA256)	www.netlock.hu/index.cgi?ca=caca
Üzleti	(SHA256)	www.netlock.hu/index.cgi?ca=cbca
Expressz	(SHA256)	www.netlock.hu/index.cgi?ca=ccca
OnlineSSL	(SHA256)	www.netlock.hu/index.cgi?ca=olsslgca

Köztes szintű kiadó, ha a kliensek csak aláírói tanúsítványtípust használnak:

Közjegyzői	(SHA256)	www.netlock.hu/index.cgi?ca=calca
Üzleti	(SHA256)	www.netlock.hu/index.cgi?ca=cblca
Expressz	(SHA256)	www.netlock.hu/index.cgi?ca=cclca

5.2. SHA 1 kiadók

Az SHA1 algoritmusú kiadók a következő URL-eken érhetők el.

Legfelső szintű kiadók:

Közjegyzői	(SHA1)	www.netlock.hu/index.cgi?ca=kozjegyzoi

5.3. Összes kiadó

Természetesen használható egy előre összeállított csomag is erre a célra, mely a következő címen érhető el (javasolt az netlock_osszes_auth_kiado.pem fájl használata a csomagból): http://www.netlock.hu/docs/letoltes/auth_kiadok_csomag.zip

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

6. Az Apache beállítása

Az Apache beállításához a következőkben ismertetett lépések szükségesek.

6.1. Kliens authentikáció bekapcsolása, elfogadott kiadók beállítása

A lépések a következők:

1. Fel kell másolni a használni kívánt CA tanúsítványokat a webszerverre, és az Apache hozzáféréséhez megfelelő jogosultságot kell adni.

2. Be kell állítani az Apache szervert arra, hogy használja a kliens tanúsítványos azonosítását.

```
#TLS hiba kizarasa konfiguraciobol
SSLInsecureRenegotiation       off

#hasznalhato kiadok megadasa
#a hivatkozott fajl a hasznalhato tanustvanyokat tartalmaza BASE64 pem formatumban
#egymas utan felsorolva
SSLCACertificateFile conf/ssl.crt/ca.crt

#a visszavonasi listak utvonalanak beallitasa
SSLCARevocationPath conf/crls

#kliens authentikacio tiltasa teljes site-ra
SSLVerifyClient      none

#ha a site-nak csak egyes reszeire akarjuk eloirni, akkor
#az altalanos konfigba „none” kerul
#SSLVerifyClient     required
#hasznalhato helyette ha az egesz site-ot igy akarjuk hasznalni
```

3. Az egyes könyvtárak viselkedését ezek után az SSLRequire és az SSLVerifyClient opciók határozzák meg.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

6.2. A visszavonási listák letöltésének és használatának beállítása

A visszavont tanúsítványok kezeléséhez az SSLCARevocationPath változóban megadott útvonalra kell letöltenie a használt kiadók visszavonási listáit, valamilyen szkript segítségével, valamint engedélyeznie kell a tűzfalon a szkript által elérendő címeket:

A letöltés ajánlott maximális gyakorisága: 2 óránként

FIGYELEM!
A szükségesnél gyakoribb letöltések esetén a NetLock DoS védelme bekapcsol, és ilyenkor a visszavonási lista letöltése az adott IP-ről rövid ideig nem lehetséges!

6.2.1. SHA 256 kiadók CRL elérése

Az SHA256 algoritmusú kiadók CRL-jei a következő URL-eken érhetők el.

Legfelső szintű kiadó:

Arany	(SHA256)	crl1.netlock.hu/index.cgi?crl=gold

Köztes szintű kiadó, ha a kliensek csak authentikációs tanúsítványtípust használnak:

Közjegyzői	(SHA256)	crl1.netlock.hu/index.cgi?crl=caca
Üzleti	(SHA256)	crl1.netlock.hu/index.cgi?crl=cbca
Expressz	(SHA256)	crl1.netlock.hu/index.cgi?crl=ccca
OnlineSSL	(SHA256)	www.netlock.hu/index.cgi?ca=olsslgca

Köztes szintű kiadó, ha a kliensek csak aláírói tanúsítványtípust használnak:

Közjegyzői	(SHA256)	crl1.netlock.hu/index.cgi?crl=calca
Üzleti	(SHA256)	crl1.netlock.hu/index.cgi?crl=cblca
Expressz	(SHA256)	crl1.netlock.hu/index.cgi?crl=cclca

6.3. SHA 1 kiadók CRL elérése

Az SHA1 algoritmusú kiadók CRL-jei a következő URL-eken érhetők el.

Legfelső szintű kiadók:

Közjegyzői	(SHA1)	crl1.netlock.hu/index.cgi?ca=kozjegyzoi

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

6.4. SSLVerifyClient

Az opció bekapcsolása esetén a szerver ragaszkodik ahhoz, hogy a kliens mutasson fel egy érvényes tanúsítványt az elfogadható tanúsítványkiadók által kiadottak közül. A kiadói tanúsítványok az SSLCACertificateFile paraméterben megadott fájlban találhatók.

```
<Location>
   SSLRequireSSL
   SSLVerifyClient require
</Location>
```

Ez a beállítás azt jelenti, hogy minden tanúsítvány elfogadható, ami érvényes és olyan tanúsítványkiadótól származik, amit korábban a konfigurációban megadtunk.

6.5. SSLRequire

Azon kívül, hogy a kliensnek érvényes tanúsítvánnyal kell rendelkeznie, megadhatók egyéb feltételek is, melyeknek teljesülnie kell.

```
 <Location>
 SSLRequireSSL
 SSLRequire %{SSL_CLIENT_S_DN_CN} in {"Varga Viktor","Kelemen Szabolcs"} \
        and %{SSL_CLIENT_S_DN_O} eq "NetLock Kft."
</Location>
```

Ebben az esetben a CN mezőben „Varga Viktor” vagy „Kelemen Szabolcs” nevet tartalmazó tanúsítvánnyal lehetséges a belépés, de csak akkor, ha a tanúsítvány O mezője a „Netlock Kft.” adatot tartalmazza.

Az egyes lehetséges szűrőfeltételeket a tanúsítvány adattartalmával kapcsolatosan a függelék tartalmazza.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

7. Form Signing

A weboldalon az SSL kliens authentikáció ideális kiegészítője a Form Signing technológia.

A Form Signing megoldás célja, hogy az on-line, kliens oldalon kitöltött, html alapú formanyomtatványok (továbbiakban: form) paraméterezhető módon, fokozott biztonságú vagy minősített elektronikus aláírással kerüljenek ellátásra, illetve megküldésre a szerver részére.

Az elektronikusan aláírt adatok védik az adat feldolgozóját a hiteles azonosítás hiányából eredő bizonytalanság, visszaélési lehetőségek, illetve a tranzakció későbbi letagadása jelentette veszély ellen.

A megoldás eleme egy szerver oldali modul is, melynek célja a hitelesített form-okhoz kapcsolódó elektronikus aláírások érvényességének ellenőrzése.

7.1. Kliens oldali aláíró modul

A kliens oldali modul célja, hogy a felhasználó Internet Explorer böngészőjébe letöltődve és ott futva (ActiveX) külön szoftver telepítése nélkül váljon lehetővé elektronikus aláírások létrehozatala a végfelhasználó tanúsítványának felhasználásával. Mivel a kliens oldali modult a NetLock kifejezetten a felhasználók 90%-a által használt Internet Explorer böngésző alá fejlesztette, illetve a Mozilla alapú - általában több operációs rendszeren is futó - böngészők (Mozilla, Netscape, Firefox) már gyárilag tartalmazzák a form signing funkcionalitást, a felhasználók legszélesebb köre számára is lehetővé válik a hiteles elektronikus ügyintézés.

Az aláírások formátuma lehet: PKCS#7 (RFC2315), XMLDSIG (RFC3275), XAdES-BES, XAdES-T, XAdES-C, XAdES-XL, XAdES-A, többszörös XAdES-A (ETSI 101903).

Mivel a szerver oldali modul támogatja a Mozilla alapú böngészők által használt PKCS#7-es aláírás-formátumot is, a szerver oldalon az aláírás ellenőrzése során nem merül fel nehézség, ha különböző böngészők által létrehozott aláírások ellenőrzése a feladat.

A fentiekből következően kliens oldali platformfüggetlenség érhető el, mely révén az elektronikus ügyintézés például Linux-os felhasználók számára is lehetővé válik.

Amennyiben ilyen megoldásra van szüksége, kérjük, keresse Vevőszolgálatunkat!

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

7.2. Szerver oldali aláírás ellenőrző modul

A szerver oldalra telepített modul feladata a kliens oldal által küldött hitelesített form-okhoz kapcsolódó, fenti formátumok valamelyikének megfelelő elektronikus aláírások érvényességének ellenőrzése. A szerver oldali modul az alábbi operációs rendszereken érhető el: NT 4.0, Windows 2000, Windows 2003, Linux, Tru64 Unix. A modul elérhető operációs rendszer-, illetve függvény szinten hívható változatban vagy PL/SQL felületen keresztül is. Amennyiben Ön más szerver oldali operációs rendszeren kívánja futtatni vagy más felületen keresztül kívánja elérni a szerver oldali modult, kérjük, hogy érdeklődjön Vevőszolgálatunknál.

7.3. A NetLock Form Signing megoldás előnyei

- Az aláírás formátumok között elérhető más böngészők által is alkalmazott formátum (PKCS#7);
- Kliens oldalon nem szükséges külön alkalmazás letöltése, telepítése, mivel a modul a böngészőben fut – ami egy felhasználóbarát megoldás;
- A kliens oldali modul kriptográfiai rétege minősített (Hung-T-024-2005.);
- A szerver oldali aláírás ellenőrző modul a legtöbb elterjedt aláírás formátum ellenőrzését támogatja;
- A szerver oldali aláírás ellenőrző modulnak a legtöbb elterjedt operációs rendszerre létezik verziója;
- A fentiek miatt mind kliens, mind szerver oldalon platformfüggetlen megoldást kínálunk;
- A megoldás használata, integrálása egyszerű.

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

8. Függelék - Egy tanúsítvány tartalma

Egy kliens authentikálásra használható tanúsítvány a következőképpen néz ki (melyből a kliens authentikálás számára a Kiadó (Issuer) és a Tárgy (Subject) sor a fontos):

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            49:dc:ff:6d:00:9b:e0:83:84:a9:88:d1:ce:cd
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:
            countryName               = HU
            localityName              = Budapest
            organizationName          = NetLock Kft.
            organizationalUnitName    = Tanúsítványkiadók (Certification Services)
            commonName                = NetLock Üzleti Eat. (Class B Legal) Tanúsítványkiadó
        Validity
            Not Before: Feb 23 15:54:28 2012 GMT
            Not After : Feb 22 15:54:28 2014 GMT
        Subject:
            countryName               = HU
            localityName              = Budapest
            organizationName          = NETLOCK Kft.
            organizationalUnitName    = Vevőszolgálat
            commonName                = Kelemen Szabolcs
            emailAddress              = kelemen.szabolcs@netlock.hu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:c1:4d:02:48:fa:38:64:6b:3a:ce:d6:51:e0:57: [. . .]
                    7f:ff
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation
            X509v3 Subject Key Identifier:
                BA:55:1B:16:6D:9E:EF:C1:0E:37:1E:C4:43:1D:4F:D4:72:80:67:13
            X509v3 Authority Key Identifier:
                keyid:34:1B:2C:C7:B2:3E:4A:72:53:3D:12:7F:40:66:BA:AE:B6:A4:E4:47
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.3555.1.38.20101201
                  CPS: http://www.netlock.hu/docs/
                  User Notice:
                    Explicit Text: Nem minősített tanúsítvány. Regisztrációkor a személyes
megjelenés kötelező. Szolgáltatási szabályzat: http://www.netlock.hu/docs/
            Authority Information Access:
                OCSP - URI:http://ocsp1.netlock.hu/cblca.cgi
                OCSP - URI:http://ocsp2.netlock.hu/cblca.cgi
                OCSP - URI:http://ocsp3.netlock.hu/cblca.cgi
                CA Issuers - URI:http://aia1.netlock.hu/index.cgi?ca=cblca
                CA Issuers - URI:http://aia2.netlock.hu/index.cgi?ca=cblca
                CA Issuers - URI:http://aia3.netlock.hu/index.cgi?ca=cblca
            X509v3 CRL Distribution Points:
                URI:http://crl1.netlock.hu/index.cgi?crl=cblca
                URI:http://crl2.netlock.hu/index.cgi?crl=cblca
                URI:http://crl3.netlock.hu/index.cgi?crl=cblca
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                email:kelemen.szabolcs@netlock.hu
    Signature Algorithm: sha256WithRSAEncryption
        1d:c6:ca:44:e2:63:04:c3:fb:08:f0:5a:0a:9c:b9:3f:bf:0d: [. . .]
        57:37:95:87
```


NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu

9. *Függelék 2 – Az SSLRequire kifejezés kliens tanúsítvánnyal kapcsolatos legfontosabb változói*

Az SSLRequire számos lehetőséget ad a szűrésre, melyekből itt csak a kliens tanúsítvánnyal kapcsolatos változókat ismertetjük. (Az egyéb változókkal kapcsolatos lehetőségekről az Apache szerver részletes dokumentációjában talál további információkat.)

Az változók neve beszédes:

SSS_CLIENT	a kliens tanúsítványára vonatkozó
_S_	a tanúsítvány subject mezője, azaz a tulajdonos adatai
_I_	a tanúsítvány issuer mezője, azaz a kiadó adatai
DN_	a tanúsítvány adattartalmára hivatkozás
C, ST, L, O, OU, CN, Email	a tanúsítvány adatmezői

SSL_CLIENT_S_DN
SSL_CLIENT_S_DN_C
SSL_CLIENT_S_DN_ST
SSL_CLIENT_S_DN_L
SSL_CLIENT_S_DN_O
SSL_CLIENT_S_DN_OU
SSL_CLIENT_S_DN_CN
SSL_CLIENT_S_DN_Email
SSL_CLIENT_I_DN
SSL_CLIENT_I_DN_C
SSL_CLIENT_I_DN_ST
SSL_CLIENT_I_DN_L
SSL_CLIENT_I_DN_O
SSL_CLIENT_I_DN_OU
SSL_CLIENT_I_DN_CN
SSL_CLIENT_I_DN_Email

NetLock Kft. cím: 1101 Budapest, Expo tér 5-7.
telefon: +36 40 22 55 22 telefax: +36 1 700 1101 e-mail: info@netlock.hu web: www.netlock.hu