

Minősített tanúsítvány, visszavonási lista és időbélyeg profildefiníciók



NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): -- 1.3.6.1.4.1.3555.1.24.20040504

A Szabályzat hatályának kezdőnapja: ----- 2004. május 4.

Oldalak száma: ----- 10, azaz tíz

© Copyright 2004, NetLock Kft. ----- Minden jog fenntartva

Jóváhagyta: ----- Rózsahegyi Zsolt ügyvezető

Jóváhagyás dátuma: ----- 2004. 05. 04.

Jóváhagyom: -----

PH.

Tartalomjegyzék

1	NETLOCK MINŐSÍTETT TANÚSÍTVÁNY- ÉS VISSZAVONÁSI LISTA KIADÓK	3
1.1	NETLOCK MINŐSÍTETT KÖZJEGYZŐI (CLASS QA) TANÚSÍTVÁNYKIADÓ	3
2	NETLOCK IDŐBÉLYEG SZOLGÁLTATÓK	4
2.1	NETLOCK MINOSITETT IDOPECSET SZOLGALTATO	4
2.2	NETLOCK MINOSITETT IDOBELYEG SZOLGALTATO	4
3	NETLOCK MINŐSÍTETT VÉGFELHASZNÁLÓI TANÚSÍTVÁNYOK	6
3.1	SZEMÉLYES ALÁÍRÓ TANÚSÍTVÁNY	6
3.2	MUNKATÁRSI ALÁÍRÓ TANÚSÍTVÁNY	7
4	NETLOCK MINŐSÍTETT VISSZAVONÁSI LISTÁK	8
5	NETLOCK MINŐSÍTETT IDŐBÉLYEG KÉRELMEK, VÁLASZOK	9
5.1	NETLOCK MINŐSÍTETT IDŐBÉLYEG KÉRELMEK	9
5.2	NETLOCK MINŐSÍTETT IDŐBÉLYEG VÁLASZOK	9
6	APPENDIX B: OBJECT IDENTIFIERS	10
6.1	ÁLTALÁNOS OID	10
6.2	NETSCAPE	10
6.3	NETLOCK	10

1 NetLock minősített tanúsítvány- és visszavonási lista kiadók

1.1 NetLock Minősített Közjegyzői (Class QA) Tanúsítványkiadó

Version: 3

Subject

Country = HU

Locality = Budapest

Organization = NetLock Halozatbiztonsagi Kft.

Organizational Unit = Tanusitvanykiadok

Common Name = NetLock Minositett Kozjegyzoi (Class QA)

Tanusitvanykiado/emailAddress=info@netlock.hu

Issuer

Country = HU

Locality = Budapest

Organization = NetLock Halozatbiztonsagi Kft.

Organizational Unit = Tanusitvanykiadok

Common Name = NetLock Minositett Kozjegyzoi (Class QA)

Tanusitvanykiado/emailAddress=info@netlock.hu

Standard extensions

- basicConstraints: critical, cA = TRUE, pathlen = 4
- keyUsage: critical, keyCertSign, cRLSign

Private extensions

- qcStatements: critical, qcCompliance
- netscape-comment: not critical, „FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgaltatasi Szabalyzataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozoz Eszkozben (BALE) keszult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgaltatasi Szabalyzatban, az Altalanos Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a <https://www.netlock.hu/docs/> cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at <https://www.netlock.hu/docs/> or by e-mail at info@netlock.net”

2 NetLock időbélyeg szolgáltatók

2.1 NetLock Minositett Idopecset Szolgáltato

Version: 3

Subject
Country = HU
Locality = Budapest
Organization = NetLock Halozatbiztonsagi Kft.
Organizational Unit = Idopecset Szolgáltatok
Common Name = NetLock Minositett Idopecset Szolgáltato

Issuer
Country = HU
Locality = Budapest
Organization = NetLock Halozatbiztonsagi Kft.
Organizational Unit = Tanusitvanykiadok
Common Name = NetLock Minositett Kozjegyzoi (Class QA)
Tanusitvanykiado/emailAddress=info@netlock.hu

Standard extensions

- basicConstraints: critical, cA = FALSE
- keyUsage: critical, nonRepudiation
- enhancedKeyUsage: timeStamping

Private extensions

- qcStatements: critical, qcCompliance
- netscape-comment: not critical, „FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgáltatasi Szabalyzataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozoz Eszkozben (BALE) keszult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgáltatasi Szabalyzatban, az Altalanos Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a <https://www.netlock.hu/docs/> cimben vagy kerhetok az info@netlock.net e-mail cimben. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at <https://www.netlock.hu/docs/> or by e-mail at info@netlock.net”

2.2 NetLock Minositett Idobelyeg Szolgáltato

Version: 3

Subject
Country = HU
Locality = Budapest
Organization = NetLock Halozatbiztonsagi Kft.
Organizational Unit = Idobelyeg Szolgáltatok
Common Name = NetLock Minositett Idobelyeg Szolgáltato

Issuer
Country = HU
Locality = Budapest

Organization = NetLock Halozatbiztonsagi Kft.
Organizational Unit = Tanusitvanykiadok
Common Name = NetLock Minositett Kozjegyzoi (Class QA)
Tanusitvanykiado/emailAddress=info@netlock.hu

Standard extensions

- basicConstraints: critical, cA = FALSE
- keyUsage: critical, nonRepudiation
- enhancedKeyUsage: timeStamping

Private extensions

- qcStatements: critical, qcCompliance
- netscape-comment: not critical, „FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Idobelyegzes Szolgaltatoi tanusitvanya. A minositett idobelyeghez a vonatkozó jogszabalyokban meghatarozott joghatasok kizarolag a Minositett Szolgaltatasi Szabalyzatban es Altalanos Szerzodesi Feltetelekben meghatarozott feltetelek mellett fuzodnek. A dokumentumok megtalalhatok a <https://www.netlock.hu/docs/> cimén vagy kerhetok az info@netlock.hu e-mail cimén. WARNING! This is a time stamping certificate of the NetLock Qualified Time Stamping Service. The use of this certificate and time stamps signed by it are subject to the NetLock Qualified CPS available at <https://www.netlock.hu/docs/> or by e-mail at info@netlock.hu.”

3 NetLock minősített végfelhasználói tanúsítványok

3.1 Személyes aláíró tanúsítvány

Mező	Tartalom
Common Name	Magánszemély neve
E-mail	Magánszemély e-mail címe vagy üres
Organization	- (üres)
Organization Unit	- (üres)
Locality	Lakcím szerinti város
State	Lakcím szerinti megye vagy üres
Country	Lakóhely szerinti ország kódja ISO 3166 szerint
Issuer	CN= NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/ O= NetLock Halozatbiztonsagi Kft./ OU= Tanusitvanykiadok/ C= HU/ L= Budapest/ ST= / E= info@netlock.hu
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Signature	Kibocsátó elektronikus aláírása

Kiterjesztések	T ¹	K	Tartalom
basicConstraints	I I	I	CA=FALSE
keyUsage	I I O	I	(Kulcshasználati jelzések) nonRepudiation (aláírás készítésére használható) digitalSignature (azonosításra használható)
qcStatements	I I O O	O	(Minősített jelzések) qcCompliance (a tanúsítvány minősített) qcLimitValue (egyszeri alkalommal vállalható értékhatár) qcRetentionPeriod (kibocsátáshoz kapcsolódó dokumentációk megőrzési ideje)
crlDistributionPoint	O	N	Kibocsátó aktuális visszavonási listájának elérése
certificatePolicies	O I O O	N	(Alkalmazott szolgáltatási szabályzat azonosítói) policyIdentifier (a szabályzat egyedi azonosítója) CPSuri (a szabályzat elérése Interneten) userNotice (megjeleníthető szabályzat kivonat)
netscapeComment	I	N	FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgaltatasi Szabaly zataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozó Eszkozben (BALE) kes zult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgaltatasi Szabalyzatban, az Altalános Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a https://www.netlock.hu/docs/ cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at https://www.netlock.hu/docs/ or by e-mail at info@netlock.net

¹ Rövidítések: T (tartalmazza), K (kritikus kiterjesztés), I (igen), N (nem), O (opcionális/választható)

3.2 Munkatársi aláíró tanúsítvány

Mező	Tartalom
Common Name	Magánszemély neve
E-mail	Magánszemély e-mail címe vagy üres
Organization	Szervezet, azaz a másodlagos alany neve
Organization Unit	Szervezeti egység neve vagy üres
Locality	Szervezet székhelye, telephelye szerinti város
State	Szervezet székhelye, telephelye szerinti megye vagy üres
Country	Szervezet székhelye, telephelye szerinti ország kódja ISO 3166 szerint
Issuer	CN= NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/ O= NetLock Halozatbiztonsagi Kft./ OU= Tanusitvanykiadok/ C= HU/ L= Budapest/ ST= / E= info@netlock.hu
Version	V3
Serial number	Egyedi sorozatszám érték
Validity	Érvényesség kezdete és vége
Public Key	Tanúsítvány tulajdonosának nyilvános kulcsa
Signature	Kibocsátó elektronikus aláírása

Kiterjesztések	T	K	Tartalom
basicConstraints	I I	I	CA=FALSE
keyUsage	I I O	I	(Kulcshasználati jelzések) nonRepudiation (aláírás készítésére használható) digitalSignature (azonosításra használható)
qcStatements	I I O O	O	(Minősített jelzések) qcCompliance (a tanúsítvány minősített) qcLimitValue (egyszeri alkalommal vállalható értékhatár) qcRetentionPeriod (kibocsátáshoz kapcsolódó dokumentációk megőrzési ideje)
crlDistributionPoint	O	N	Kibocsátó aktuális visszavonási listájának elérése
certificatePolicies	O I O O	N	(Alkalmazott szolgáltatási szabályzat azonosítói) policyIdentifier (a szabályzat egyedi azonosítója) CPSuri (a szabályzat elérése Interneten) userNotice (megjeleníthető szabályzat kivonat)
netscapeComment	I	N	FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Szolgaltatasi Szabaly zataban leirt eljarasok alapjan keszult. A kibocsatott tanusitvanyhoz tartozo magankulcs a jogszabalyi rendelkezeseknek megfelelo Biztonsagos Alairas Letrehozoz Eszkozben (BALE) kes zult. A minositett elektronikus alairas joghatas ervenyesulesenek, valamint elfogadasanak feltetele a Minositett Szolgaltatasi Szabalyzatban, az Altalános Szerzodesi Feltetelekben eloirt ellenorzesi eljaras megtetele. A dokumentumok megtalalhatok a https://www.netlock.hu/docs/ cimem vagy kerhetok az info@netlock.net e-mail cimem. WARNING! This certificate has been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance and the use of this certificate are subject to the NetLock Qualified CPS available at https://www.netlock.hu/docs/ or by e-mail at info@netlock.net

4 NetLock minősített visszavonási listák

Mező	Tartalom
Version	V2
Issuer	CN= NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/ O= NetLock Halozatbiztonsagi Kft./ OU= Tanusitvanykiadok/ C= HU/ L= Budapest/ ST= / E= info@netlock.hu
thisUpdate	CRL érvényesség kezdete
nextUpdate	CRL érvényesség vége
Signature	Kibocsátó elektronikus aláírása

Visszavonási információk	T	K	Tartalom
userCertificate	I		Az érvénytelen tanúsítványok sorozatszama
revocationDate	I		Az érvénytelenítés időpontja
crlEntryExtensions	I	O	(érvénytelenítés értelmezései)
	O		<i>CRLReason</i> (érvénytelenítés okának kódja)
	O		<i>holdInstruction</i> (tennivaló felfüggesztéskor)
	O		<i>invalidityDate</i> (valószínűsíthető érvénytelenségi idő)

5 NetLock minősített időbélyeg kérelmek, válaszok

5.1 NetLock minősített időbélyeg kérelmek

Mezők, tulajdonságok	Tartalom, értelmezés
A kérelemben engedélyezett hash algoritmusok	SHA-1 vagy RIPEMD160
Kérelemben megnevezhető szabályzati azonosító (OID)	Üresen hagyható vagy a kért szabályzat azonosítója
Kérelemben szereplő véletlen szám (nonce) hossza	Maximum 64 bit
Időbélyeg kérelemben kérhető-e a szolgáltató tanúsítványa (certReq)	Igen

5.2 NetLock minősített időbélyeg válaszok

Mezők, tulajdonságok	Tartalom, értelmezés
Időbélyeg válaszban szereplő szabályzati azonosító (OID)	A kért (vagy ha nem volt ilyen a kérelemben, úgy az aktuális) szabályzat azonosítója
Az időbélyeg válasznál használt hash algoritmus	SHA1 vagy RIPEMD160
Az időbélyeg válasznál használt aláíró algoritmus	RSA
Verzió	V1
Sorszám mérete	Dinamikus hosszúságú
Sorszám egyedisége	Az időbélyegzőben használt sorszám egyedi a Szolgáltatóra nézve. Ez a tulajdonság ésszerű keretek között fennmarad a szolgáltatás lehetséges megszakadása után is.

Kiterjesztések	T	K	Tartalom
NL_TS_ext1	O	N	NetLock privát kiterjesztés ügyfélspecifikus céllal

6 APPENDIX B: Object Identifiers

6.1 *Általános OID*

```
id-ce OBJECT IDENTIFIER ::= {Joint ISO/ITU-T assignment(2) X.500 Directory
Services(5) certificateExtension (29)}
keyUsage OBJECT IDENTIFIER ::= {id-ce 15}
basicConstraints OBJECT IDENTIFIER ::= {id-ce 19}
certificatePolicies OBJECT IDENTIFIER ::= {id-ce 32}
enhancedKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
```

```
qcStatements OBJECT IDENTIFIER ::= {itu-t(0) identified-
organization(4) etsi(0) id-qc-profile(1862) 1}
qcCompliance OBJECT IDENTIFIER ::= {qcStatements 1}
qcLimitValue OBJECT IDENTIFIER ::= {qcStatements 2}
qcRetentionPeriod OBJECT IDENTIFIER ::= {qcStatements 3}
```

6.2 *Netscape*

```
netscape OBJECT IDENTIFIER ::= {Joint ISO/ITU-T assignment(2) Joint
assignments by country(16) USA(840) US company arc(1) Netscape
Communications Corp.(113730)}
netscape-cert-extension OBJECT IDENTIFIER ::= {netscape 1}
netscape-cert-type OBJECT IDENTIFIER ::= {netscape-cert-extension 1}
netscape-comment OBJECT IDENTIFIER ::= {netscape-cert-extension 13}
```

6.3 *NetLock*

```
id-netlock OBJECT IDENTIFIER ::= {iso(1) identified-organization(3) dod(6)
internet(1) private(4) enterprise(1) netlock(3555)}
id-netlock-techspec OBJECT IDENTIFIER ::= {id-netlock techspec(3)}
NL_TS_ext1 OBJECT IDENTIFIER ::= {id-netlock-techspec TS_ext1(1)}
```