Minősített tanúsítvány, visszavonási lista és időbélyeg profildefiníciók

NetLock Informatikai és Hálózatbiztonsági Korlátolt Felelősségű Társaság

Nyilvántartási szám (OID): -- 1.3.6.1.4.1.3555.1.24.20050815

A Szabályzat hatályának kezdőnapja: ---- 2005. augusztus 15.

Oldalak száma: ------------------------- 12, azaz tizenkettő

Jóváhagyta: ---------------------- Rózsahegyi Zsolt ügyvezető

Jóváhagyás dátuma: --------------------- 2005. augusztus 15.

Jóváhagyom: --

PH.

Tartalomjegyzék

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 Letrehozo 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.hudocs/ or by e-mail at info@netlock.net”

2 NetLock időbélyeg szolgáltatók

2.1 NetLock Minositett Idopecset Szolgaltato

Version: 3

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

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
- extendedKeyUsage: critical, timeStamping

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 Letrehozo 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.hudocs/ or by e-mail at info@netlock.net”

2.2 NetLock Minositett Idobelyeg Szolgaltato

Version: 3

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

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
- extendedKeyUsage: critical, timeStamping

Private extensions

- qcStatements: critical, qcCompliance
- netscape-comment: not critical, „FIGYELEM! Ezen tanusitvany a NetLock Kft. Minositett Idobelyegzes Szolgaltatoi tanusitvanya. A minositett idobelyeghez a vonatkozo 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/ cimen vagy kerhetok az info@netlock.hu e-mail cimen. 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 OCSP válasz aláírók

3.1 NetLock OCSP Kiszolgalo

Version: 3

Subject
Country = HU
Locality = Budapest
Organization = NetLock Kft.
Organizational Unit = Visszavonasi Szolgaltatosok
Common Name = NetLock OCSP Kiszolgalo

Issuer
Country = HU
Locality = Budapest
Organization = NetLock Halozatbiztonsagi Kft.
Organizational Unit = Tanusitvanykiadok
Common Name = NetLock Expressz (Class C) Tanusitvanykiado

Standard extensions

- basicConstraints: critical, cA = FALSE
- keyUsage: critical, digitalSignature, keyEncipherment, keyAgreement
- extendedKeyUsage: OCSP Signing
- ocspNoCheck: not critical

4 NetLock minősített végfelhasználói tanúsítványok

4.1 Személyes aláíró tanúsítvány

Mező	Tartalom
Common Name	Magánszemély neve, álnevet tartalmazó tanúsítvány esetén "ALNEV„ előtét, illetve az elfogadott álnév
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	(Kulcshasználati jelzések)
	I		*nonRepudiation (aláírás készítésére használható)*
qcStatements	I	O	(Minősített jelzések)
	I		*qcCompliance (a tanúsítvány minősített)*
	O		*qcLimitValue (egyszeri alkalommal vállalható értékhatár)*
	O		*qcRetentionPeriod (kibocsátáshoz kapcsolódó dokumentációk megőrzési ideje)*
	O		*qcSSCD (a privát kulcs BALE-ban használandó*
authorityKeyID	O	N	Kibocsátó kulcsára vonatkozó információ
subjectKeyID	O	N	Alany kulcsára vonatkozó információ
crlDistributionPoint	O	N	Kibocsátó aktuális visszavonási listájának elérése
certificatePolicies	I	N	(Alkalmazott szolgáltatási szabályzat azonosítói)
	I		*policyIdentifier (a szabályzat egyedi azonosítója)*
	O		*CPSuri (a szabályzat elérése Interneten)*
	O		*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 Letrehozo Eszkozben (BALE) kes zult. 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.h u/docs/ cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate ha s been issued as a qualified certificate. The corresponding private key has been generated on a Secure Signature Creation Device (SSCD). The issuance

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

Kiterjesztések	T[1]	K	Tartalom
			and the use of this certificat e are subject to the NetLock Qualified CPS available at https://www.netlock.hu/docs/ or by e-mail at info@netlock.net

4.2 Munkatársi aláíró tanúsítvány

Mező	Tartalom
Common Name	Magánszemély neve
E-mail	Magánszemély e-mail címe vagy üres
Title	Magánszemély titulusa 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	(Kulcshasználati jelzések)
	I		*nonRepudiation (aláírás készítésére használható)*
qcStatements	I	O	(Minősített jelzések)
	I		*qcCompliance (a tanúsítvány minősített)*
	O		*qcLimitValue (egyszeri alkalommal vállalható értékhatár)*
	O		*qcRetentionPeriod (kibocsátáshoz kapcsolódó dokumentációk megőrzési ideje)*
	O		*qcSSCD (a privát kulcs BALE-ban használandó*
authorityKeyID	O	N	Kibocsátó kulcsára vonatkozó információ
subjectKeyID	O	N	Alany kulcsára vonatkozó információ
crlDistributionPoint	O	N	Kibocsátó aktuális visszavonási listájának elérése
certificatePolicies	I	N	(Alkalmazott szolgáltatási szabályzat azonosítói)
	I		*policyIdentifier (a szabályzat egyedi azonosítója)*
	O		*CPSuri (a szabályzat elérése Interneten)*
	O		*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 Letrehozo Eszkozben (BALE) kes zult. 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.h u/docs/ cimen vagy kerhetok az info@netlock.net e-mail cimen. WARNING! This certificate ha s been issued as a qualified certificate. The corresponding private key has been generated on a

Kiterjesztések	T	K	Tartalom
			Secure Signature Creation Device (SSCD). The issuance and the use of this certificat e are subject to the NetLock Qualified CPS available at https://www.netlock.hu/docs/ or by e-mail at info@netlock.net

5 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 sorozatszáma
revocationDate	I		Az érvénytelenítés időpontja
crlEntryExtensions	I	O	(érvénytelenítés értelmezései)
	O		*CRLReason (érvénytelenítés okának kódja)*
	O		*holdInstruction (tennivaló felfüggesztéskor)*
	O		*invalidityDate (valószínűsíthető érvénytelenségi idő)*

6 NetLock minősített időbélyeg kérelmek, válaszok

6.1 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

6.2 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

7 APPENDIX B: Object Identifiers

7.1 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}
```

7.2 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}
```

7.3 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)}
```