Az Educatio Társadalmi Szolgáltató Közhasznú Társaság elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásának tanúsítvány-profilja

v 3.7

Időpont	Jóváhagyta	Aláírás
2007.	Kerekes Gábor	

Időpont	Készítette	Aláírás
2007. június 29.	Sóti András Tóth Elemér	

Változáskövetés

Időpont	**Referencia**	**Tartalom**
2006. május 1.	Tóth Elemér	első változat
2006. május 30.	Tóth Elemér, Babócsy László	v2: Az EuroOne Rt-vel egyeztetett második változat
2006. június 3.	Babócsy László	Az EuroOne Rt által átadott, MS Windows CA-t követő módosításokat tartalmazó változat
2007. június 29.	Tóth Elemér, Sóti András	v3: A nyilvános CA szolgáltatáshoz kapcsolódó változat, egyeztetve a MÁV INFORMATIKA Kft-vel (Benkó Tamással és Kővári Ferenccel).
2007. július 26.	Tóth Elemér, Sóti András	ügyfélhez kapcsolódó o= és ou= beállítások módosítása; CRL profil
2007. augusztus 3.	Tóth Elemér, Sóti András	v3.3: User Notice módosítása (max. 200 karakterre)
2007. augusztus 29.	Tóth Elemér, Sóti András	v3.4: álnév használatának pontosítása
2007. szeptember 3.	Tóth Elemér	v3.5: certificate policies extension megváltoztatása (9A táblázat); ser.n. és surname CA-nál; egyeztetés MÁV INFORMATIKA Kft-vel (Benkó Tamással, illetve Kővári Ferenccel)
2007. szept. 12.	Tóth Elemér	v3.6: szolgáltatói tanúsítványadatok és CRL issuer adatok módosítása a Kht nevének megadása miatt, valamint az Authority Info Acc. megadása
2007. nov.30.	Tóth Elemér	v3.7: „álneves tanúsítványok” tervként történő megadása

Tartalom

Táblázatok jegyzéke

1. A dokumentum célja

Jelen dokumentumban Educatio Társadalmi Szolgáltató Közhasznú Társaság (továbbiakban: Educatio Kht.) által az elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatás számára meghatározott és alkalmazott tanúsítvány és visszavonási lista struktúrák, valamint beállítások kerültek rögzítésre.

A CA konfigurálását az Educatio Kht. cert-admin szerepkörrel felruházott munkatársa, ezen dokumentumot felhasználva végzi el.

Ezt a dokumentumot nem kell nyilvánosan publikálni, de kérésre be lehet mutatni az érdeklődő kliensek és partnerek, valamint az Eat-ban megjelölt Hatóság számára.

2. Referenciák

A tanúsítvány profilok tervezése az alábbi dokumentumokra támaszkodik:

- IETF/PKIX RFC 3280/4325update Certificate and Certificate Revocation List (CRL) Profile,
- ETSI TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
- Az IHM ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára (2005. november)
- a magyarországi hitelesítés szolgáltatói gyakorlatra.

3. Felépítés

A dokumentum követi a fenti 2. pontban megadott IHM ajánlás felépítését.

4. A tanúsítványok egységes szerkezete és közös adattartalma

Valamennyi tanúsítvány az alábbi általános szerkezetet követi (M – kötelező, O – opcionális, F – tiltott; I – kitöltendő, N – nem kell kitölteni; +C – kritikus, -C – nem kritikus beállítás):

Mező/Attribútum	Kötelező			Kitöltendő			Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O		
TBSCertificate	X			X				részletezve a 2. táblázatban
signature Algorithm								
(algorithm)	X			X			sha1RSA	OID: 1.2.840.113549.1.1.5
(algorithm) parameters		X			X			sha1RSA-nak nincs!
signatureValue	X			X			az aláírás értéke	legalább 256 bájt

1. táblázat A tanúsítványok általános szerkezete és elvárt közös adattartalma

Mező/Attribútum	Kötelező			Kitöltendő			Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O		
TBSCertificate								
Version	X			X			V3	(V3!)
serialNumber	X			X			<CA generált adat>	
signature	X			X			sha1RSA	OID: 1.2.840.113549.1.1.5
issuer	X							egyedi név (dn=)
country				X			„HU”	ország azonosító; /UTF8 kódolással/
organization				X			**<ld. a 2A. táblázatban>**	a kibocsátó CA szervezet neve
organization-unit						X	<nincs>	CA részlegének neve
distinguised name qualifier					X		<nincs>	
state or province					X		<nincs>	
common name				X			**<ld a 2A. táblázatban>**	márkanév (!)
serial number					X		<nincs>	IHM v15ec V1.2: nem
locality					X		<nincs>	
title					X		<nincs>	
surname					X		<nincs>	
given name					X		<nincs>	
initials					X		<nincs>	
pseudonym					X		<nincs>	
generation qualifier					X		<nincs>	
Validity	X			X				
notBefore							<a kiadás dátuma és időpontja>	UTCTime
notAfter							< a tanúsítvány érvényességi időtartama>	UTCTime
Subject	X			X			**<részletezve a 6. táblázatban>**	A végfelhasználó adatai
subjectPublicKeyInfo	X			X				
algorithm								RSA (legalább 1024 bites kulccsal); OID: 1.2.840.113549.1.1.
subjectPublicKey								A végfelhasználó nyilvános kulcsa
issuerUniqueID			X		X		<nincs>	
subjectUniqueID			X		X		<nincs	
extensions		X		X			**<részletezve a 3. táblázatban>**	

2. táblázat: A TBSCertificate részletes szerkezete és elvárt adattartalma

Mező/Attribútum	Kötelező			Kitöltendő			Zártkörű CA	Nyilvános CA
	M	O	F	I	N	O		
organization				X			„OFIK”	„Educatio Társadalmi Szolgáltató Kht” /Printable string kódolás/
organization-unit						X	<nincs>	<nincs>
common name				X			„Educatio Társadalmi Szolgáltató Közhasznú Társaság”	„EDUCA-2”

2A. táblázat: A szolgáltatói név megadása

Mező/Attribútum	Kötelező			Kitöltendő			Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O		
extensions								
Standard Extensions		X		X			**<részletezve a 4. táblázatban>**	
Internet Certificate Extensions		X		X			**<részletezve a 5. táblázatban>**	
Qualified Certificates Profile Extensions			X		X			

3. táblázat A kiterjesztések (extensions) általános szerkezete

Mező/Attribútum	Kötelező			Kitöltendő			Kritikus		Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O	+C	-C		
Standard extensions										
AuthorityKeyIdentifier										
keyIdentifier		X		X				X	<CA által generált adat>	Meg kell egyeznie a tanúsítványt kibocsátó CA megfelelő szolgáltatói tanúsítványának subject key identifier értékével.
authorityCertIssuer		X			X			X	<nincs>	
authorityCertSerial Number		X			X			X	<nincs>	
SubjectKeyIdentifier keyIdentifier	X			X				X	<CA által generált adat>	
KeyUsage	X			X			X		**<részletezve a 8. táblázatban>**	
PrivateKeyUsagePeriod			X		X			X	<nincs>	
Certificate Policies	X			X				X	**<részletezve a 9. táblázatban>**	
PolicyMappings		X			X			X	<nincs>	

SubjectAltName										
otherName		X			X			X		
rfc822Name		X		X				X	felhasznalonev@domain.hu	e-mail cím
dNSName		X			X			X		
x400Address		X			X			X		
directoryName		X			X			X		
ediPartyName		X			X			X		
uniformResourceIdentifier		X			X			X		
iPAddress		X			X			X		
registeredID		X			X			X		
IssuerAltName		X			X			X		
SubjectDirectoryAttributes		X			X			X		
BasicConstraints cA	X			X			X		FALSE	Végfelhasználói (és nem szolgáltatói) tanúsítványok esetén: FALSE
NameConstraints			X		X			X	<nincs>	Csak szolgáltatói tanúsítványokban lehet használni!
PolicyConstraints		X			X			X	<nincs>	
ExtKeyUsage		X		X				X	**<részletezve a 10. táblázatban>**	
CRLDistributionPoints distributionPoint		X		X				X	**<ld. 4A. táblázat>**	A CRL-fájl elérési helye.
inhibitAnyPolicy		X			X			X	<nincs>	
FreshestCRL		X			X			X	<nincs>	

4. táblázat: a Standard extensions részletes szerkezete és elvárt közös adattartalma

Mező/Attribútum	Kötelező			Kitöltendő			Kritikus		Zártkörű CA	Nyilvános CA
	M	O	F	I	N	O	+C	-C		
CRLDistributionPoints distributionPoint		X		X				X	URL=http://crl.pkica1.educatio.hu/certenroll/educatio-ca1.crl	URL=http://crl.pkica2.educatio.hu/certenroll/educatio-ca2.crl

4A. táblázat: A CRL fájl elérési helye

Mező/Attribútum	Kötelező			Kitöltendő			Kritikus		Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O	+C	-C		
Private Internet Extensions										
[1] Authority Information Access		X		X				X		
accessMethod									**<Ld. 5A. táblázat>**	a tanúsítványkiadói tanúsítvány hozzáférésének OID-je
accessLocation									**<Ld. 5A. táblázat>**	
[2] Authority Information Access		X		X				X		
accessMethod									<nincs>	OCSP esetén megadandó OID
accessLocation									<nincs>	OCSP esetén megadandó
Subject Information Access		X				X		X	<a Szolgáltató által generált adat>	

5. táblázat: a Private Internet Extensions részletes szerkezete és elvárt közös adattartalma

Mező/Attribútum	Kötelező			Kitöltendő			Kritikus		Zártkörű CA	Nyilvános CA
	M	O	F	I	N	O	+C	-C		
[1] Authority Information Access										
accessMethod										1.3.6.1.5.5.7.48.2
accessLocation									URL=http://crl.pkica1.educatio.hu/certenroll/educatio-ca1.crt	URL=http://crl.pkica2.educatio.hu/certenroll/educatio-ca2.crt

5A. táblázat: accessLocation megadása

Időjelzés szolgáltatás esetén az accessLocation mezőben szerepelnie kell a szolgáltatás elérési címének (http/ftp esetén URI; TCP/IP esetén dNSName, vagy ipAddress).

5. A különböző tanúsítványok különös adattartalma

Az ügyfelekhez tartozó tanúsítványok profilja (az álnév használatát a Hitelesítés szolgáltatási Szabályzat 3.1.3 pontja szerint kell kezelni!):

Mező/Attribútum	Kötelező			Kitöltendő			Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O		
subject	X							egyedi név (dn=)
country							**<Ld. 6A. táblázat>**	ország azonosító
organization				X			**<Ld. 6A. táblázat>**	az ügyfelekhez rendelt szervezet neve; a köztisztviselőknél a képviselt szervezet neve
organization-unit						X	**<Ld. 6A. táblázat>**	ha van; a szolgáltatói tanúsítványoknál „IT admins” megjelölés
distinguised name qualifier					X		<nincs>	
state or province					X		<nincs>	
common name				X			az ügyfél neve	Valós név esetén: az ügyfél (RO, SO DÜ is!) neve, mely betű szerint azonos a regisztráció alapjául szolgáló igazolványban foglalt névvel, szóköz elválasztójel(eke)t és az UTF8 kódolással. Álnév használata esetén: a megadott név előtt és mögött ~ (tilde) karaktert helyez el a regisztrációs munkatárs.
serial number				X			**<Ld. 6A. táblázat>**	A betű szerint azonos common name mezőtartalommal rendelkező ügyfelek megkülönböztetését szolgáló egyedi sorszám, melyet a hitelesítés-szolgáltató generál.
locality					X		<nincs>	város/falu
title						X	<nincs>	„dr.”
surname							**<Ld. 6A. táblázat>**	A common name mező azon része, mely az ügyfél/ügyintéző vezetéknevének tekintendő.
given name					X		<nincs>	A given name (amennyiben pl. adatbázisoknál erre szükség van) már származtatható: a common name azon része, mely a surname mező tartalmát egészíti ki.

initials					X		<nincs>	
pseudonym					X		<nincs>	
generation qualifier					X		<nincs>	

6. táblázat Ügyfelek tanúsítványának subject beállítása

Mező/Attribútum	Kötelező			Kitöltendő			Zártkörű CA	Nyilvános CA
	M	O	F	I	N	O		
subject								
country	X			X			<nincs>	„HU”
organization	X					X	<nincs>	szervezet, ha az ügyfél kéri; köztisztviselők esetén: közigazgatási szerv megadása kötelező! ; a szolgáltatói tanúsítványoknál „Educatio Társadalmi Szolgáltató Kht.”megjelölés
organization-unit	X					X	pedagógus-azonosító, vagy „IT admins”	osztály/részleg, ha az ügyfél kéri; köztisztviselők esetén: szervezeti egység, ha a meghatalmazás tartalmazza; a szolgáltatói tanúsítványoknál „IT admins” megjelölés
serial number	X			X			<nincs>	Valós név esetén: oktatási-azonosító (sorszám), opcionális
								Álnév használata esetén: a már létező álnév megkülönböztetését jelző szám.
surname	X			X			<nincs>	Valós név esetén: vezetéknév
		X			X		<nincs>	Álnév használata esetén: üres
domain component						X	„educatio”	
domain component						X	„cadomain”	

6A. táblázat Ország azonosító és az ügyfelekhez rendelt virtuális szervezet megjelölése

Megjegyzés: LDAP-fa építése: dc=HU, dc=EDUCA-2

Az Educatio Kht. valamely web-szerveréhez tartozó tanúsítványok:

Mező/Attribútum	Kötelező			Kitöltendő			Elvárt adattartalom	Megjegyzés
	M	O	F	I	N	O		
subject	X							
country				X			„HU”	ország azonosító
organization				X			„Educatio Társadalmi Szolgáltató Kht.”	a szervert üzemeltető szervezet neve
organization-unit						X		az üzemeltető részlegének neve
distinguised name qualifier					X		<nincs>	
state or province					X		<nincs>	
common name							**<Ld. 7A. táblázat>**	A szerver DNS szerinti, vagy egyéb módon hitelesített elnevezése, szóköz elválasztójel(eke)t és az UTF-8 kódolással.
serial number					X		<nincs>	
locality					X		„Budapest”	
title					X		<nincs>	
surname					X		<nincs>	
given name					X		<nincs>	
initials					X		<nincs>	
pseudonym					X		<nincs>	
generation qualifier					X		<nincs>	

7. táblázat: A szerver tanúsítványok subject beállítása

Mező/Attribútum	Kötelező			Kitöltendő			Zártkörű CA	Nyilvános CA
	M	O	F	I	N	O		
common name							„pkica1.educatio.hu”	

7A. táblázat: A szerver tanúsítványok subject beállítása

Extended Key – SMIME Capability a WEB szerver tanúsítványban -- TERV

Certificate Extensions: 9
1.2.840.113549.1.9.15: Flags = 0, Length = 37

Mező/Attribútum	OID	Parameters
SMIME Capabilities [1]	1.2.840.113549.3.2	02 02 00 80
SMIME Capabilities [2]	1.2.840.113549.3.4	02 02 00 80
SMIME Capabilities [3]	1.3.14.3.2.7	
SMIME Capabilities [4]	1.2.840.113549.3.7	

7B. táblázat: SMIME Capability - web szerver tanúsítvány kiterjesztésének adattartalma

A kulcs-felhasználás beállításai a közoktatási zártkörű szolgáltatás esetén:

Mező/Attribútum	Felhasználói hitelesítés célú (authentikációs) tanúsítványok		Letagadhatatlanság célú (aláíró) tanúsítványok	Titkosítás célú tanúsítványok -- TERV	
	Személy számára	SSL-szerver számára	Nem minősített elektronikus aláíráshoz	Személy számára	VPN szerver számára
KeyUsage					
digitalSignature	**<beállítva>**	**<beállítva>**			
nonRepudiation					
keyEncipherment		**<beállítva>**			
dataEncipherment					
keyAgreement					
keyCertSign					
cRLSign					
encipherOnly					
decipherOnly					

8. táblázat: A különböző tanúsítványok KeyUsage kiterjesztésének adattartalma

A kulcs-felhasználás beállításai a felsőoktatási zártkörű szolgáltatás esetén:

Mező/Attribútum	Felhasználói hitelesítés célú (authentikációs) tanúsítványok		Letagadhatatlanság célú (aláíró) tanúsítványok	Titkosítás célú tanúsítványok -- TERV	
	Személy számára	SSL-szerver számára	Nem minősített elektronikus aláíráshoz	Személy számára	VPN szerver számára
KeyUsage					
digitalSignature		**<beállítva>**	**<beállítva>**		
nonRepudiation			**<beállítva>**		
keyEncipherment		**<beállítva>**			
dataEncipherment					
keyAgreement					
keyCertSign					
cRLSign					
encipherOnly					
decipherOnly					

8A. táblázat: A különböző tanúsítványok KeyUsage kiterjesztésének adattartalma

A kulcs-felhasználás beállításai a nyilvános szolgáltatás esetén:

Mező/Attribútum	Felhasználói hitelesítés célú (authentikációs) tanúsítványok		Letagadhatatlanság célú (aláíró) tanúsítványok	Titkosítás célú tanúsítványok -- TERV	
	Személy számára	SSL-szerver számára	Nem minősített elektronikus aláíráshoz	Személy számára	VPN szerver számára
KeyUsage					
digitalSignature		**<beállítva>**	**<beállítva>**		
nonRepudiation			**<beállítva>**		
keyEncipherment		**<beállítva>**			
dataEncipherment					
keyAgreement					
keyCertSign					
cRLSign					
encipherOnly					
decipherOnly					

8B. táblázat: A különböző tanúsítványok KeyUsage kiterjesztésének adattartalma

A kulcs-felhasználás beállításai az időjelzés szolgáltatás esetén: digitalSignature és nonRepudiation beállítva.

Mező/Attribútum	Zártkörű CA Ügyfelekhez tartozó tanúsítvány	Zártkörű CA Educatio Kht. valamely szerveréhez tartozó tanúsítvány	Nyilvános CA
Certificate Policies			
[1] Certificate Policy	CertPolicyID		
[1,1]Policy QualifierInfo: policy QualifierId qualifier	Policy Qualifier Id=CPS , Qualifier OID: 1.3.6.1.4.1.311.21.8.7425865.10907826.14762115.2257285.15158098.82.4077818.15191963		<Ld. 9A táblázat>
	http://crl.pkica1.educatio.hu/szabalyzatok/default.asp	http://crl.pkica1.educatio.hu/szabalyzatok/default.asp	<Ld. 9A táblázat>
[1,2]Policy QualifierInfo: policy QualifierId qualifier	UserNotice: „”	UserNotice: „”	<Ld. 9A táblázat>

9. táblázat: a különböző tanúsítványok Certificate Policies kiterjesztésének elvárt adattartalma

Mező/Attribútum	Nyilvános CA ügyfelekhez tartozó tanúsítvány	Nyilvános CA köztisztviselőhöz tartozó tanúsítvány	Nyilvános CA nem közig.ügyfél tanúsítványa - TERV
Certificate Policies			
[1] Certificate Policy	OID: 0.2.216.1.100.42.101.3.2.1	OID: 0.2.216.1.100.42.101.4.2.1	OID: 1.3.6.1.4.1.27537.1.1
[1,1]Policy QualifierInfo: policy QualifierId qualifier	Policy Qualifier Id=CPS , Qualifier OID: 1.3.6.1.5.5.7.2.1 http://educa2.educatio.hu/szabalyzatok/EducatioHSZSZ.pdf		
[1,2]Policy QualifierInfo: policy QualifierId qualifier	UserNotice: „A tanúsítvány közigazgatási ügyfél számára készült, értelmezése az Educatio Kht. által alkalmazott hitelesítési rend (HR) és HSZSZ szerint. A KGYHSZ felelőssége kizárva a saját HR-je szerint.” (191)	UserNotice: „A tanúsítvány tulajdonosa köztisztviselő, értelmezése az Educatio Kht. által alkalmazott hitelesítési rend (HR) és HSZSZ szerint. A KGYHSZ felelőssége kizárva a saját HR-je szerint.” (181)	UserNotice: ”A tanúsítvány a közigazgatásban nem használható, értelmezése az Educatio Kht. által alkalmazott hitelesítési rend (HR) és HSZSZ szerint.” ()

Megjegyzés: a UserNotice-ban megadott szöveg mögötti zárójeles szám az időzőjelbe tett UserNotice szöveg hosszát adja meg, karakterekben számolva. Ez a szám 200 alatt kell legyen.

9A. táblázat: a különböző tanúsítványok Certificate Policies kiterjesztésének elvárt adattartalma

Hitelesítési rend OID-k:
- közig. ügyfélhez -- OID: 0.2.216.1.100.42.101.3.2.1
- közig. köztisztviselőhöz -- OID: 0.2.216.1.100.42.101.4.2.1
- nem közigazgatási ügyfélhez -- OID: 1.3.6.1.4.1.27537.1.1

Dokumentumok jelzése:
http://educa2.educatio.hu/szabalyzatok/EducatioHSZSZ.pdf -- közig. ügyfélhez, köztisztviselőhöz, nem közigazgatási ügyfélhez tartozó HSZSZ dokumentum megadása.

Mező/Attribútum	Zártkörű CA Felhasználói hitelesítés célú (authentikációs) tanúsítványok		Zártkörű CA Letagadhatatlanság célú (aláíró) tanúsítványok	Zártkörű CA Titkosítás célú tanúsítványok	
	Személy számára	SSL-szerver számára	Nem minősített elektronikus aláíráshoz tartozó tanúsítvány	Személy számára	VPN szerver számáa
ExtKeyUsage					
keyPurposeID	TLS Client Auth	serverAuth	Secure Email	<nincs>	<nincs>
keyPurposeID	<nincs>	<nincs>	<nincs>	<nincs>	<nincs>

OID:

TLS Client Auth	1.3.6.1.5.5.7.3.2	SCLogon	1.3.6.1.4.1.311.20.2.2
serverAuth	1.3.6.1.5.5.7.3.1	clientAuth	1.3.6.1.5.5.7.3.2
Secure Email	1.3.6.1.5.5.7.3.4	IPsec end sys	1.3.6.1.5.5.7.3.5
		IP sec IKE i.m.	1.3.6.1.5.5.8.2.2

10. táblázat: a különböző tanúsítványok ExtKeyUsage kiterjesztésének elvárt adattartalma

Mező/Attribútum	Felhasználói hitelesítés célú (authentikációs) tanúsítványok		Letagadhatatlanság célú (aláíró) tanúsítványok	Titkosítás célú tanúsítványok	
	Személy számára	SSL-szerver számára	Nem minősített elektronikus aláíráshoz tartozó tanúsítvány	Személy számára	VPN szerver számáa
ExtKeyUsage					
keyPurposeID	TLS Client Auth	serverAuth	Secure Email	Secure Email	IPsec end sys
keyPurposeID	SCLogon	clientAuth	<nincs>	<nincs>	IP sec IKE

10A. táblázat: a különböző tanúsítványok ExtKeyUsage kiterjesztésének elvárt adattartalma

Időjelzés szolgáltatás esetén szerepelnie kell az id-kp-timeStamping OID (1.3.6.1.5.5.7.3.8) értéknek.

6. Visszavonási lista (CRL) profil

Az alábbi táblázatban szereplő jelölések: +C – kritikus, -C – nem kritikus beállítás.

Mező	Kritikus		Nyilvános CA	Megjegyzés
	+C	-C		
Version			1	Verzió szám: 2, az RFC 3280 ajánlás alapján.
Signature Algorithm Identifier			SHA-1	Algoritmus azonosító.
Signature				Szolgáltató visszavonási listát hitelesítő elektronikus aláírása.
Issuer			c=”HU”, o=” Educatio Társadalmi Szolgáltató Kht.”, cn=”EDUCA-2”	A visszavonási listát kibocsátó hitelesítő egység egyedi azonosítója. A visszavonási listát az adott hitelesítő egység a tanúsítványok aláírására használt kulcsával hitelesíti.
Effective Date				A visszavonási lista hatályba lépésének kezdete, RFC 3280 szerinti kódolással.
Next Update				Következő kibocsátás ideje, 3280 szerinti kódolással.
Revoked Certificates				A visszavont tanúsítványok listája a tanúsítvány sorozatszámával és a visszavonás idejével.
Bejegyzési információk				
Reason Code		X		Visszavonás oka.
Invalidity Date		X		Érvénytelenség ideje.
Hold Instruction		X		Felfüggesztett tanúsítvány jelzése.

11. táblázat: CRL profil és tartalma