Anexa Profile la
Codul de Practici și Proceduri certSIGN
SSL DV CA Clasa 3 G2
pentru certificate SSL DV

Versiunea 1.22

Data: 15 Ianuarie 2026

Notă importantă

Adresa: Bulevardul Tudor Vladimirescu nr. 29 A,
AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901

Web:www.certsign.ro

Istoric document

Vers.	Data Efectivă[1]	Motiv	Persoana care a făcut schimbarea
1.18	Iulie 2023	Publicarea primei versiuni	Manager politici PKI
1.19	Ianuarie 2024	Revizuire anuală	Manager Politici PKI
1.20	15 Ianuarie 2025	Revizuire anuală	Manager Politici PKI
1.21	15 Aprilie 2025	Actualizare footer	Manager Politici PKI
1.22	15 Ianuarie 2026	Revizuire anuală	Manager Politici PKI

Acest document a fost aprobat de

Versiune	Nume	Data
1.18	Comitetul de Management al Politicilor si Procedurilor	Iulie 2023
1.19	Comitetul de Management al Politicilor si Procedurilor	Ianuarie 2024
1.20	Comitetul de Management al Politicilor si Procedurilor	Ianuarie 2025
1.21	Comitetul de Management al Politicilor si Procedurilor	Aprilie 2025
1.22	Comitetul de Management al Politicilor si Procedurilor	Ianuarie 2026

Cuprins

[1] *Data efectivă este ultima zi a lunii*

7 Profil certificate, CRL și OCSP

Profilurile de certificate și profilul Listă de revocare a certificatelor (CRL) sunt conforme cu formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerințele RFC 6960. Informațiile enumerate mai jos descriu semnificația câmpurilor de certificat respective, CRL și OCSP, standarde aplicate și extensii private utilizate de CERTSIGN.

7.1 Profilul certificatului

certSIGN SSL DV CA Class 3 G2 îndeplinește cerințele tehnice stabilite în CABF BR secțiunea 2.2 - Publicarea informațiilor, secțiunea 6.1.5 - Dimensiunile cheilor și secțiunea 6.1.6 - Generarea parametrilor cheii publice și verificarea calității.
Câmpul SerialNumber este un număr nesecvențial mai mare decât zero (0) și mai mic de 2^{159}, care conține cel puțin 64 de biți de la un CSPRNG.
Toate obiectele semnate de o cheie privată certSIGN CA sunt conforme cu cerințele CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului AlgorithmIdentifier-derivat în contextul semnăturilor.
Câmpul SubjectPublicKeyInfo indică o cheie RSA utilizând identificatorul de algoritm rsaEncryption (OID: 1.2.840.113549.1.1.1.1), cu un parametru NULL explicit.
AlgorithmIdentifier pentru cheile RSA TREBUIE să fie identic, octet cu octet, cu următorii octeți codificați hexagonal: 300d06092a864886f70d0101010500.
Pentru ECDSA, se vor utiliza identificatorii și codificările specificate în #7.1.3.2 din CABF BR.

Profilul certificatului CA subordonat

Toate denumirile subiecților sunt codificate conform specificațiilor din secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.10.2 "CA Certificate Naming" din CABF BR.
Profilul câmpurilor de bază pentru certificatul certSIGN SSL DV CA Clasa 3 G2 este descris în Tabelul 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	20060516700317887a0be0d34ac3af	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN ROOT CA
	Organization (O) =	certSIGN
	Country (C) =	RO
Not before (validity period beginning date)	Jan 30 09:44:44 2018 GMT	
Not after (validity period end date)	Jan 30 09:44:44 2028 GMT	
Subject (Distinguished Name)	Common Name (CN) =	certSIGN SSL DV CA Class 3 G2
	Organisation Unit (OU) =	certSIGN SSL DV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
Subject Public Key Info	2048 bits RSA key	

Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)

Tabelul 7.1. Profilul câmpurilor de bază pentru certSIGN SSL DV CA Clasa 3 G2

Profilul certificatului de end-user (server)

Câmpul notBefore are o valoare în termen de max 48 de ore de la operațiunea de semnare a certificatului.

Toate denumirile subiecților sunt codificate în conformitate cu CABF BR secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.7.2 "Domain Validated".

Atributul "Subscriber Certificate Common Name" conține exact o intrare care este una dintre valorile conținute în extensia subjectAltName a certificatului, codificată ca o copie caracter cu caracter a valorii intrării dNSName din extensia subjectAltName. În mod specific, toate etichetele de domeniu ale porțiunii Fully-Qualified Domain Name sau FQDN din Wildcard Domain Name vor fi codificate ca etichete LDH, iar etichetele P NU vor fi convertite în reprezentarea lor Unicode.

Profilul câmpurilor de bază pentru certificatele DV emise de certSIGN SSL DV CA Clasa 3 G2 este descris în Tabelul 7.2.

Field name	Value or value's constraint	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN SSL DV CA Class 3 G2
	Organisational Unit (OU) =	certSIGN SSL DV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains fields countryName & commonName, as presented in Chapter 7.1.4.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Tabelul 7.2. Profilul câmpurilor de bază ale certificatelor DV emise de certSIGN SSL DV CA Clasa 3 G2

Profilul de precertificat

Un precertificat este identic din punct de vedere structural cu un certificat de server pentru utilizatorul final, cu excepția unei extensii speciale de „otrăvire" critică în câmpul extensions, cu OID-ul 1.3.6.1.4.1.11129.2.4.3, și este creat după ce CA-ul a decis să emită un certificat, dar înainte de semnarea efectivă a certificatului.

Câmpurile de bază ale precertificatului:
- **version** codificată este identică, octet cu octet, cu câmpul "versiune" din certificat.
- **serialNumber** codificată este identică, octet cu octet, cu câmpul serialNumber din certificat (ca o excepție de la RFC 5280, secțiunea 4.1.2.2).
- **signature** codificată este identică, octet cu octet, cu câmpul de semnătură din certificat.
- **issuer** codificată este identică, octet cu octet, cu câmpul issuer din certificat.
- **validity** codificată este identică, octet cu octet, cu câmpul validity al certificatului.
- **subject** codificată codificată este identică, octet cu octet, cu câmpul "subject" al certificatului.
- **subjectPublicKeyInfo** codificată codificată este identică, octet cu octet, cu câmpul subjectPublicKeyInfo din certificat.
- **issuerUniqueID** Encoded value este identic octet cu octet cu câmpul issuerUniqueID din certificat sau este omis dacă este omis în certificat.
- **subjectUniqueID** codificată este identică octet cu octet la octet cu câmpul subjectUniqueID din certificat sau este omisă dacă este omisă în certificat.

Field name	Value or value's constraint for Precertificates	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN SSL DV CA Class 3 G2
	Organisational Unit (OU) =	certSIGN SSL DV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
Not before	Universal Time Coordinated based.	
Not after	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains countryName and commonName fields.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Profilul de certificat OCSP Responder
CA emitentă a respondentului este aceeași cu CA emitentă pentru certificatele pentru care furnizează răspunsuri.

Field name	Value or value's constraint for OCSP Responder	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN SSL DV CA Class 3 G2
	Organisational Unit (OU) =	certSIGN SSL DV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
Not before	Universal Time Coordinated based.	
Not after	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains countryName and commonName fields.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

7.1.1 Număr de versiune

Toate certificatele emise de CERTSIGN sunt X.509 versiunea 3.

7.1.2 Extensii de certificate

Extensiile profilelor de certificat sunt în conformitate cu CABF BR nr. 7.1.2 "Certificate Content and Extensions".

Extensii ale profilului de certificat de CA subordonat

AuthorityInfoAccess conține una sau mai multe AccessDescriptions. Fiecare AccessDescription conține doar o AccessMethod permisă, iar fiecare AccessLocation este codificată ca tip GeneralName specificat.
Extensia **Authority Key Identifier** conține doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al autorității de certificare emitente.
CA Certificate **Basic Constraints**: cA set TRUE; pathLenConstraint setat la 0 sau NULL.
Extensia **Certificate Policies** conține cel puțin o "PolicyInformation", care conține exact un identificator rezervat al politicii de certificat - pentru certificatele CA emise după 2023.
Extensia **CRL Distribution Points** conține cel puțin un DistributionPoint, de tip uniformResourceIdentifier, iar schema fiecăruia este "http". Primul *GeneralName* conține URL-ul HTTP al serviciului CRL al CA emitente pentru certificatul CA.
certSIGN CA generează un **subjectKeyIdentifier** care este unic în cadrul tuturor certificatelor pe care le-a emis pentru fiecare cheie publică unică.
Pentru certificatele CA emise după 2023 - CA Certificate **Extended Key Usage** conține id-kp-serverAuth key și, opțional, id-kp-clientAuth.

Extensiile de certificate pentru certSIGN SSL DV CA Clasa 3 G2 sunt descrise în Tabelul 7.3.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.certsign.ro/certcrl/root.crt	Non-critical
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critical
Authority Key Identifier	e0 8c 9b db 25 49 b3 f1 7c 86 d6 b2 42 87 0b d0 6b a0 d9 e4	Non-critical
Subject Key Identifier	f5 dc bb fb 89 1e ca 78 81 74 6c b6 4a 6c 25 4d 54 81 7e 06	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.1.1.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/root.crl	Non-critical

Tabelul 7.3. Extensii ale certificatului certSIGN SSL DV CA Clasa 3 G2

Extensii ale profilului de certificat de end-user (server)

AuthorityInfoAccess conține una sau mai multe AccessDescriptions. Fiecare AccessDescription conține doar o AccessMethod permisă, iar fiecare AccessLocation este codificată ca fiind de tipul GeneralName specificat.
Extinderea **Authority Key Identifier** conține doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al CA emitente.
Extensia **Certificate Policies** conține cel puțin un "PolicyInformation" și conține exact un singur identificator de politică de certificat rezervat:
{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain- validated(1)}(**2.23.140.1.2.1**)
The permitted **policyQualifiers**, id-qt-cps (OID: 1.3.6.1.5.5.7.2.1), URL HTTP sau HTTPS pentru declarația privind practicile de certificare a autorității de certificare emitente.
End-user DV Certificate **Extended Key Usage** conține cheia id-kp-serverAuth și, opțional, id-kp-clientAuth.
Subject Alternative Name este prezent și conține cel puțin un dNSName. dNSName conține fie un nume de domeniu complet calificat, fie un nume de domeniu cu caractere wildcard pe care CA l-a validat în conformitate cu secțiunea 3.2.2.4 din CABF BR. Numele de domeniu wildcard sunt validate în conformitate cu secțiunea 3.2.2.2.6 din CABF BR. Intrarea dNSName nu conține un nume intern. Numele de domeniu complet calificat sau porțiunea FQDN a

numelui de domeniu wildcard conținută în intrare este compusă în întregime din etichete P sau etichete LDH nerezervate, unite între ele printr-un caracter U+002E FULL STOP (".").
Eticheta de domeniu de lungime zero care reprezintă zona rădăcină a sistemului de nume de domeniu Internet NU este inclusă.

Valori de utilizare a cheilor (***Key Usage)***: digitalSignature și keyEncipherment.

Extensia **CRL Distribution Points** conține cel puțin un DistributionPoint, de tip uniformResourceIdentifier, iar schema fiecăruia este "http". Primul GeneralName conține URL-ul HTTP al serviciului CRL al CA emitente pentru certificatul CA.

Certificatul DV SSL conține extensiile descrise în Tabelul 7.4.

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.certsign.ro/certcrl/root.crt	Non-critical
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)	Critical
Authority Key Identifier	f5 dc bb fb 89 1e ca 78 81 74 6c b6 4a 6c 25 4d 54 81 7e 06	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=2.23.140.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.1.1.5.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-ssldv.crl	Non-critical
Subject Alternative Name	This extension MUST contain at least one entry. Each entry MUST be either a DNS Name containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. Wildcard FQDNs are permitted.	Non-critical
Enhanced Key	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical

Extension	Value or Value constraint	Extension status
Usage	Client Authentication (1.3.6.1.5.5.7.3.2)	

Tabelul 7.4. certSIGN SSL DV CA Clasa 3 G2 extensii certificate end-user

Extensiile profilului de precertificat
Precertificatul conține extensia "Precertificate Poison" (OID:1.3.6.1.4.1.11129.2.4.3). Această extensie are o valoare OCTET STRING care este exact octetul 0500, reprezentarea codificată a valorii ASN.1 NULL, astfel cum este specificată în RFC 6962, secțiunea 3.1.

Extensii ale profilului de certificat OCSP Responder
Extensia Authority Key Identifier are doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al autorității de certificare emitente.
OCSP Responder Extended Key Usage este doar OCSP Signing (1.3.6.1.5.5.5.7.3.9).certSIGN include extensia id-pkix-ocsp-nocheck (OID: 1.3.6.1.5.5.5.7.7.48.1.5).
Această extensie are un extnValue OCTET STRING care este exact octetul 0500 codificat hexagonal, reprezentarea codificată a valorii NULL ASN.1, astfel cum este specificat în RFC 6960, secțiunea 4.2.2.2.2.2.1.
OCSP Responder Key Usage este doar digitalSignature.
subjectAltName, authorityInformationAccess, certificatePolicies, crlDistributionPoints nu sunt stabilite ca extensii pentru certificatele OCSP emise după 2023.

Certificatul OCSP conține extensii descrise în tabelul 7.5.

Extension	Value or Value constraint	Extension status
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)[2]	Critical
Authority Key Identifier	65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41	Non-critical
Subject Key Identifier	3c 76 7c 4a 3c 2d 6c 5a 82 c0 2d 62 f9 2e 17 89 e5 55 f0 b6	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck	-	Non-critical

Tabelul 7.5. Extensii de certificate OCSP

7.1.3 Identificatori de algoritm obiect

SubjectPublicKeyInfo
Câmpul SubjectPublicKeyInfo indică o cheie RSA folosind identificatorul de algoritm rsaEncryption (OID: 1.2.840.113549.1.1.1.1), cu un parametru NULL explicit.

[2] nonRepudiation (bit 1) is not permitted for OCSP certificates issued after 15-Sep-2023

AlgorithmIdentifier pentru cheile RSA este identic, octet cu octet, cu următorii octeți codificați hexagonal: 300d06092a864886f70d0101010500.
Pentru ECDSA, se vor utiliza identificatorii și codificările specificate în #7.1.3.1.1.2 din CABF BR.

Identificatorul algoritmului de semnătură
Toate obiectele TLS semnate de o cheie privată certSIGN CA sunt conforme cu cerințele din CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului AlgorithmIdentifier-derivat în contextul semnăturilor. În cazul certSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.1.11).

7.1.4 Forme de nume

Codificarea numelui
Conținutul câmpurilor din certificatele DV trebuie să îndeplinească cerințele din secțiunea 3.1 și din ultima versiune publicată a CAB Forum Baseline Requirements Certificate Policy.

Numele Emitentului, pentru toate căile de certificare posibile, trebuie să fie identic octet-cu-octet cu Numele Subiectului din certificatul emitentului. Atributele Subiectului nu pot conține doar metadate precum ‘.’, ‘-’, și ’ ’ (adică spațiu) pentru a indica faptul că valoarea nu există, este incompletă, sau nu este aplicabilă.

Pentru fiecare cale de certificare validă (conform definiției din RFC 5280, secțiunea 6):
- Pentru fiecare certificat din calea de certificare, conținutul codificat al câmpului Issuer Distinguished Name al unui certificat este identic, octet cu octet, cu forma codificată a câmpului Subject Distinguished Name al certificatului CA emitent.
- Pentru fiecare certificat TLS CA din calea de certificare, conținutul codificat al câmpului Subject
Distinguished Name al unui certificat este identic octet cu octet între toate certificatele ale căror Subject Distinguished Names pot fi comparate ca fiind egale în conformitate cu RFC 5280, secțiunea 7.1, inclusiv certificatele expirate și revocate.

Codificarea TLS Subject
Atributele din câmpul subiect al certificatului vor fi codificate și poziționate în conformitate cu tabelul 77: "Cerințe de codificare și ordine pentru atributele selectate" din secțiunea 7.1.4.2 Codificarea atributelor subiectului din CABF BR.

Atributul "Subscriber TLS Certificate Common Name"
Acest atribut conține exact o intrare care reprezintă una dintre valorile conținute în extensia subjectAltName a certificatului.
În cazul în care valoarea este un nume de domeniu complet calificat sau un nume de domeniu wildcard, atunci valoarea este codificată ca o copie, caracter cu caracter, a valorii intrării dNSName din extensia extensia subjectAltName. Mai exact, toate etichetele de domeniu ale unui domeniu complet calificat (Fully-Qualified Domain Labels) Name sau FQDN din partea Wildcard Domain Name trebuie să fie codificate ca etichete LDH, iar etichetele P NU vor fi convertite în reprezentarea lor Unicode.

7.1.5 Constrângeri de nume

Nu se aplică.

7.1.6 Identificator de obiect al politicii de certificat

Identificatorii obiectelor politicii certificatelor utilizate la nivelul certSIGN SSL DV CA Clasa 3 G2 sunt descriși în Tabelul 7.6 și Tabelul 7.7.

Certification Policy Name	Policy identifier
certSIGN SSL DV CA Class 3 G2	***{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1)*** **{certSIGN} .{id-policy}(1). {id-cp}(1).{id-DV-CA}(5) . *subpolicy ID=1.3.6.1.4.1.25017.1.1.5. subpolicy ID*** See below table for *subpolicyID* values.

Tabelul 7.6. Identificatorii de politici și numele acestora pentru certificatele certSIGN SSL DV CA Clasa 3 G2

CA Level	OID
certSIGN SSL DV CA Class 3 G2 1.3.6.1.4.1.25017.1.1.5	*DV certificate for website authentication* - ***.1*** *OCSP certificate* - ***.2***

Tabelul 7.7 Identificatori de obiecte de politică de certificat

7.1.7 Utilizarea extensiei de constrângeri de politică

Nu se aplică.

7.1.8 Sintaxa și semantica calificativelor de politici

CERTSIGN emite certificate cu un calificativ de politică în cadrul extensiei Politici de certificat. Această extensie conține un calificator de pointer CPP care indică CPP.

7.1.9 Prelucrarea semanticii pentru extensia critică de politici de certificat

Nu se aplică.

7.2 Profil CRL

certSIGN CA utilizează o CRL completă și integrală, adică o CRL a cărei sferă de aplicare include toate certificatele emise de CA.

Câmpul **nextUpdate** indică data până la care va fi emisă următoarea CRL. Pentru CRL-urile care acoperă certificatele de abonat, cel mult 10 zile după **thisUpdate**. Pentru celelalte CRL, la cel mult 12 luni de la thisUpdate.

Câmpul **revokedCertificates** este prezent dacă CA a emis un certificat care a fost revocat și dacă intrarea corespunzătoare nu a apărut încă în cel puțin o CRL programată în mod regulat după perioada de valabilitate a certificatului revocat. CA va elimina o intrare pentru un certificat corespunzător după ce acesta a apărut în cel puțin o CRL programată periodic după perioada de valabilitate a certificatului revocat.

Profilul CRL este descris în Tabelul 7.8.

Field name	Value or value's constraint	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Common Name (CN) =	certSIGN SSL DV CA Class 3 G2
	Organisational Unit (OU) =	certSIGN SSL DV CA Class 3 G2
	Organization (O) =	certSIGN
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	
NextUpdate	Date of next expected CRL update	
Revoked Certificates	List of revoked certificates	

Tabelul 7.8 Profil CRL pentru certSIGN SSL DV CA Clasa 3 G2

7.2.1 Numere de versiune

Toate CRL-urile emise de CERTSIGN sunt X.509 versiunea 2.

7.2.2 CRL și extensii de intrare CRL

Extensia **CRLNumber** conține un număr INTEGER mai mare sau egal cu zero (0) și mai mic de 2^{159} și transmite o secvență strict crescătoare.
Extensiile CRL pentru certSIGN SSL DV CA Clasa 3 G2 sunt descrise în Tabelul 7.9.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical

Tabelul 7.9. Extensii CRL pentru certSIGN SSL DV CA Clasa 3 G2

serialNumber este identic, octet cu octet, cu serialNumber conținut în certificatul revocat.
revocationDate este data și ora la care a avut loc revocarea.
CA actualizează data revocării într-o intrare CRL atunci când se stabilește că cheia privată a certificatului a fost compromisă înainte de data revocării care este indicată în intrarea CRL pentru certificatul respectiv. Datarea inversă a câmpului revocationDate reprezintă o excepție de la cele mai bune practici descrise în RFC 5280 (secțiunea 5.3.2); câmpul revocationDate sprijină implementările TLS care procesează câmpul revocationDate ca fiind data la care certificatul este considerat pentru prima dată ca fiind compromis.

Extension	Value or Value constraint	Extension status
serialNumber	serialNumber of the revoked certificate	Non-critical
revocationDate	date of the certificate compromission/revocation	Non-critical
crlEntryExtensions	reason for revocation	Non-critical
CRL Reason	*Revocation reason code*	*Non-critical*

Extensiile de intrare CRL (crlEntryExtensions) acceptate de certSIGN conțin următoarele câmpuri:

ReasonCode: codul motivului revocării. Acest câmp nu este critic, permițând determinarea motivului revocării certificatului. Sunt permise următoarele motive pentru revocarea certificatului:

1. Nici un motiv furnizat sau nespecificat (RFC 5280 CRLReason # 0)
   - În cazul în care codurile de motiv nu se aplică cererii de revocare, solicitantul NU TREBUIE să furnizeze un alt cod de motiv decât "nespecificat".
2. KeyCompromise (RFC 5280 CRLReason # 1)
   - Beneficiarul certificatului TREBUIE să aleagă motivul revocării "keyCompromise" atunci când are motive să creadă că cheia privată a certificatului său a fost compromisă, de exemplu, o persoană neautorizată a avut acces la cheia privată a certificatului său.
3. AffiliationChanged (RFC 5280 CRLReason # 3)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "affiliationChanged" atunci când numele subiectului sau alte informații privind identitatea subiectului din certificat s-au schimbat, dar nu există niciun motiv pentru a suspecta că cheia privată a certificatului a fost compromisă.
4. Superseded (RFC 5280 CRLReason # 4)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "superseded" atunci când certificatul este înlocuit deoarece: abonatul a solicitat un nou certificat, CA are dovezi rezonabile că nu ar trebui să se bazeze pe validarea autorizării sau controlului domeniului pentru orice nume de domeniu complet calificat sau adresă IP din certificat, sau CA a revocat certificatul din motive de conformitate, cum ar fi faptul că certificatul nu este conform cu cerințele de bază sau cu CPS ale CA.).
5. CessationOfOperation (RFC 5280 CRLReason # 5)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "cessationOfOperation" atunci când site-ul web certificat este închis înainte de expirarea certificatului sau dacă Beneficiarul nu mai deține sau nu mai controlează numele de domeniu din certificat înainte de expirarea certificatului..
6. privilegeWithdrawn (RFC 5280 CRLReason #9)[3]
   - PrivilegeWithdrawn este destinat să fie utilizat atunci când a existat o infracțiune de partea abonatului care nu a dus la keyCompromise, cum ar fi abonatul certificatului a furnizat informații înșelătoare în cererea lor de certificat sau nu și-a respectat obligațiile materiale în temeiul acordului de abonat sau al termenilor de utilizare.

   Contractul de abonat informează abonații cu privire la opțiunile privind motivele de revocare enumerate mai sus și oferă explicații cu privire la momentul în care trebuie aleasă fiecare opțiune. Modelele de cereri de revocare, pe care AC le pune la dispoziția abonatului, permit ca aceste opțiuni să fie ușor de specificat în momentul în care abonatul solicită revocarea certificatului său, valoarea implicită fiind aceea că nu este furnizat niciun motiv de revocare [adică valoarea implicită corespunde la CRLReason "unspecified (0)", ceea ce are ca rezultat faptul că nu este furnizată nicio extensie reasonCode în CRL].

[3] *privilegeWithdrawn nu trebuie să fie pus la dispoziția abonatului ca o opțiune motiv de revocare, deoarece utilizarea acestui motiv este determinată de operatorul CA și nu de abonat*

7.3 Profil OCSP

Protocolul de verificare a stării certificatului on-line (OCSP) permite evaluarea stării certificatului.

Serviciul OCSP este furnizat de CERTSIGN în numele tuturor autorităților de certificare afiliate. Serverul OCSP, care emite confirmări de stare a certificatului, folosește o pereche de chei speciale pentru fiecare CA Intermediarși CA ROOT, generată exclusiv în acest scop.

Certificatul de server OCSP conține extensia extKeyUsage, descrisă în RFC 5280.

Această extensie este setată ca non-critică și înseamnă că o autoritate de certificare care emite certificatul către serverul OCSP confirmă prin semnarea delegării autorizației de a emite conformitatea stării certificatului (a beneficiarilor acestei autorități).

De asemenea, certificatul de server OCSP conține extensia OCSPNoCheck, descrisă de RFC 6960. Această extensie este declarată necritică ceea ce înseamnă că un client OCSP primește un răspuns semnat cu cheia privată asociată acestui certificat poate avea încredere în starea certificatului de server OCSP, fără a fi necesar să îi verificăm starea de revocare.

Entitatea care primește o confirmare emisă de serverul OCSP trebuie să accepte formatul de răspuns standard cu identificatorul id-pkix-ocsp-basic.

Informațiile despre starea certificatului sunt incluse în câmpul certStatus al structurii SingleResponse. Aceasta poate avea una dintre următoarele trei valori principale:

- GOOD - indică starea validă a certificatului

- REVOKED - indică faptul că certificatul a fost emis și revocat sau certificatul nu a fost emis în conformitate cu RFC 6960

- UNKNOWN - indică faptul că nu există suficiente informații pentru a determina starea certificatului

Când răspunsul OCSP conține un cod de eroare (mesaj), răspunsul nu este semnat digital (RCF 6960).

7.3.1 Numere de versiune

Serverul OCSP care operează în cadrul CERTSIGN emite confirmări ale stării certificatului în conformitate cu RFC 6960. Singura valoare admisibilă a numărului de versiune este 0 (este un echivalent al versiunii v1).

7.3.2 Extensii OCSP

În conformitate cu RFC 6960, serverul CERTSIGN OCSP acceptă următoarea extensie:

Nonce- legarea unei cereri și a unui răspuns pentru a preveni atacurile de răspuns. **Nonce** este inclus în **requestExtension** al **OCSPRequest** și repetat în câmpul **responseExtension** al **OCSPResponse**.