Anexa Profile la
Codul de Practici și Proceduri
certSIGN ROOT CA

Versiunea 1.45
Data: 15 Ianuarie 2026

Notă importantă

Adresa: Bd. Tudor Vladimirescu, nr. 29 A,
AFI Tech Park 1, București 050881, România

Telefon: 004-021-31.19.901

Web: www.certsign.ro

Istoria documentului

Versiune	Data Efectivă[1]	Motiv	Persoana care a făcut modificarea
1.40	Iulie 2023	Prima versiune	Manager Politici PKI
1.41	August 2023	Eliminare emailProtection	Manager Politici PKI
1.41a	Ianuarie 2024	Revizie anuală	Manager Politici PKI
1.42	18 Aprilie 2024	Adăugare certificat încrucișat	Manager Politici PKI
1.43	15 Ianuarie 2025	Actualizare cf. CABF BR	Manager Politici PKI
1.44	15 Aprilie 2025	Actualizare footer	Manager Politici PKI
1.45	15 Ianuarie 2026	Revizie anuală	Manager Politici PKI

Acest document a fost aprobat de

Versiune	Nume	Data
1.40	Comitetul de Management al Politicilor si Procedurilor	Iulie 2023
1.41a	Comitetul de Management al Politicilor si Procedurilor	Ianuarie 2024
1.43	Comitetul de Management al Politicilor si Procedurilor	Ianuarie 2025
1.44	Comitetul de Management al Politicilor si Procedurilor	Aprilie 2025
1.45	Comitetul de Management al Politicilor si Procedurilor	Ianuarie 2026

Cuprins

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

7 Profilul certificatelor, CRL și OCSP

Profilul certificatelor și al Listei de certificate Revocate (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerinţele RFC 6960. Informaţiile de mai jos descriu semnificaţia câmpurilor din certificat, CRL și OCSP, standardul aplicat și extensiile folosite de certSIGN.

7.1 Profilul certificatelor

Conform standardului X.509 v.3, un certificat este alcătuit din următoarea secvenţă de câmpuri: corpul certificatului (tbscertificate), informaţii despre algoritmul folosit pentru semnarea certificatului (signatureAlgorithm), și semnatura electronica propriu-zisă a Autorităţii de Certificare (signatureValue).

7.1.1 Numarul versiunii

Conţinutul certificatului include câmpuri de bază și extensii (standard - descrise de norme și private – definite de autoritatea emitentă).

Extensiile definite într-un certificat conform normelor permit adăugarea de atribute suplimentare specifice Beneficiarului și cheii publice și simplifică managementul structurii ierarhice a certificatului. certificatele emise în conformitate cu standardul X.509 v.3 permit definirea unor extensii proprietar, unice pentru o implementare dată.

certSIGN acceptă următoarele câmpuri de bază:

Version: a treia versiune (X.509 v.3) a formatului de certificat,

SerialNumber: numărul serial al certificatului, unic în cadrul domeniului Autorităţii de Certificare,

signatureAlgorithm: identificatorul algoritmului de semnatura folosit de Autoritatea de Certificare emitentă,

Issuer: numele distinctiv (ND) al Autorităţii de Certificare ,

Validity: perioada de validitate, descrisă prin intermediul unei date de începere (notBefore) și a unei date de expirare (notAfter) a certificatului,

Subject: numele distinctiv (ND) al Beneficiarului care este subiectul certificatului,

SubjectPublicKeyInfo: valoarea cheii publice împreună cu identificatorul algoritmului criptografic folosit.

În certificatele emise de certSIGN, valorile câmpurilor de mai sus sunt stabilite în concordanţă cu regulile descrise în Tabelul 7.1.

Numele câmpului	Valoarea sau restricţiile valorii	
Version	Versiunea 3	
Serial Number	Valoare unică pentru toate certificatele emise de Autoritățile de Certificare din cadrul certSIGN .In acest camp va fi introdusa o valoare aleatoare de 8 bytes. Pentru generarea acestei valori va fi folosit un modul criptografic hardware.	
SIGNature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Numele (CN) =	certSIGN {CA Class {1,2,3,4}}
	Departament (OU)=	certSIGN {CA Class {1,2,3,4}}
	Organizaţia (O) =	certSIGN
	Ţara (C) =	RO
Not before (data de începere a perioadei de validitate)	În baza sistemului universal de referinţă temporala (Universal Time Coordinated). certSIGN poseda un ceas controlat de Atomic Frequency Standard.	
Not after (data de expirare a perioadei de validitate)	În baza sistemului universal de referinţă temporala (Universal Time Coordinated). certSIGN poseda un ceas controlat de Atomic Frequency Standard.	
Subject (Distinguished Name)	Numele distinctiv respectă cerinţele standardului X.501. Valorile unora dintre atributele acestor câmpuri sunt opţionale și semnificaţia lor este descrisa mai jos.	
Subject Public Key Info	Criptat în conformitate cu RFC 3280, poate conține informaţii despre cheile publice ale RSA, DSA sau ECDSA (identificatorul cheii, mărimea cheii în biţi și valoarea cheii publice); mărimea cheii RSA este prezentată în Capitolul 6.1.5.	
Signature	Semnatura certificatului, generată și criptată în conformitate cu cerinţele descrise în RFC 3280.	

Tabel 7.1. Profilul câmpurilor de baza ale certificatelor

Profilele tuturor certificatelor (câmpurile din Subject):

Profilul certificatului CA subordonat
Toate denumirile subiecților sunt codificate conform specificațiilor din CABF BR secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.10.2 "CA Certificate Naming".

Profilul de certificat al CA subordonate cu certificare încrucișată
Acest profil de certificat este utilizat la emiterea unui certificat de CA care utilizează același nume de subiect și informații despre cheia publică a subiectului ca unul sau mai multe certificate CA subordonate existente.

7.1.2 Extensia certificatelor

Rolul fiecărei extensii este definit de valoarea standard a identificatorului de obiect folosit (**OBJECT IDENTIFIER**). Extensia, funcţie de opţiunea autorităţii emitente, poate fi **critică** sau **ne-critică**. Dacă o extensie este definită ca fiind **critică**, aplicaţia care foloseşte certificatul trebuie să respingă orice certificat care conține o extensie critică nerecunoscută. Pe de altă parte, extensiile definite ca fiind **ne-critice** pot fi omise.
certSIGN acceptă următoarele câmpuri de extensii standard:

- **AuthorityKeyIdentifier**: identificatorul certificatului de cheie publică al Autorităţii de Certificare, asociat cheii private folosită pentru semnarea certificatelor – **această extensie nu este critică**,
- **SubjectKeyIdentifier** – identificatorul cheii Beneficiarului - această extensie nu este critică,
- **KeyUsage**: scopul în care poate fi folosită cheia - **această extensie este critică**. Extensia descrie pentru ce poate fi utilizată o cheie, de exemplu, pentru criptarea de date, pentru schimbul de date, pentru semnarea electronica etc.:
  - **digitalsignature** (0) – cheie pentru crearea de semnaturi electronice
  - **nonRepudiation** (1) – cheie asociată cu serviciile de ne-repudiere
  - **keyEncipherment** (2) – cheie pentru schimbul de chei,
  - **dataEncipherment** (3) – cheie pentru criptarea datelor
  - **keyAgreement** (4) – cheie pentru negocierea de chei
  - **keycertsign** (5) – cheie pentru semnarea de certificate
  - **CRLsign**(6) – cheie pentru semnarea de CRL-uri
  - **encipherOnly** (7) – cheie numai pentru criptare
  - **decipherOnly** (8) – cheie numai pentru decriptare
- **ExtKeyUsage**: defineşte restricţiile cu privire la folosirea cheii - **extensia nu este critică**. Acest câmp defineşte unul sau mai multe domenii de utilizare posibilă a certificatului, adiţional domeniilor standard, definite de câmpul **KeyUsage**. Acest câmp trebuie înţeles ca o restrângere a scopurilor permise definite în câmpul **keyUsage**. certSIGN emite certificate care pot conține una dintre următoarele valori sau o combinaţie de astfel de valori în câmpul ExtKeyUsage:
  - **serverAuth** - autentificarea serverelor web TLS; biții de câmp **keyUsage** sunt setați pentru: digitalSignature, keyEncipherment sau keyAgreement
  - **clientAuth** – autentificarea clienţilor Web TLS; **keyUsage** are setaţi biţii pentru: digitalsignature și /sau keyAgreement;
  - **codesigning** – semnarea codurilor executabile; **keyUsage** are setat bitul pentru digitalsignature;
  - **emailProtection** – protecția e-mail-ului; **keyUsage** are setaţi biţii pentru: digitalsignature, non-Repudiation și/sau (keyEncipherment sau keyAgreement),
  - **ipsecEndSystem** – protocolul de protecţie IPSEC,
  - **ipsecTunnel** – protocolul IPSEC Tunnelling,
  - **ipsecUser** – protocolul de protecţie IP al aplicaţiilor utilizatorului,
  - **timeStamping** – legarea rezumatului (digest) cu timpul furnizat de sursa de încredere**; keyUsage** are setaţi biţii pentru: digitalSIGNature, nonRepudiation.

- **OCSPsigning** – asignează dreptul de a emite confirmări privind starea certificatului în numele lui CA; keyUsage are setaţi biţii pentru: digitalsignature, nonRepudiation.
- **dvcs** – emiterea unei confirmări de către un notar autorizat, pe baza protocolului DVCS; keyUsage are setaţi biţii pentru: digitalSignature, nonRepudiation, keycertSIGN, cRLSIGN.
- **EncryptedFileSystem** – permite folosirea certificatului pentru criptarea sistemului de fişiere (EFS); este cerut obligatoriu de anumite aplicaţii de acest gen (ex. EFS);
- **SmartCardLogon –** permite utilizarea certificatului pentru operaţia de „smart-card logon" - autentificare în sistemul de operare, bazată pe certificat digital;

- **Certificate Policies** – extensia indică politica (politicile) sub care va emite certificate o Autoritate de Certificare sau politica (politicile) sub care a fost emis un certificat de către o Autoritate de Certificare. Extensia este o listă de **PolicyInformation** – informaţii (identificatorul, adresa electronica) despre o politică de certificare aplicată. **Această extensie nu este critică**.

Numele Politicii de certificare	Identificatorul Politicii
certSIGN Clasa 1	{certSIGN}[2] .{id-policy}[2]. {id-cp}[3].{id-Class-1}[4] =1.3.6.1.4.1.25017.1.1.1
certSIGN Clasa 2	{certSIGN} id-policy(1) id-cp(1)id-Class-2(2)= 1.3.6.1.4.1.25017.1.1.2
certSIGN Clasa 3	{certSIGN} id-policy(1) id-cp(1)id-Class-3(3) =1.3.6.1.4.1.25017.1.1.3
certSIGN Clasa 4	{certSIGN} id-policy(1) id-cp(1)id-Class-4(4) =1.3.6.1.4.1.25017.1.1.4

Tabelul 7.1.2 Identificatorii politicilor și numele acestora

Certificatele emise de către Autoritățile de Certificare includ și calificatori, recomandaţi de RFC 3280 :

- **PolicyMapping**: map-area politicii – **acest câmp nu este critic**; acest câmp conține una sau mai multe perechi de OID, definind echivalenţa politicii emitentului certificatului cu politica Beneficiarului certificatului,
- **SubjectAlternativeName:** numele alternativ al Beneficiarului– acest câmp nu este critic;
- **BasicConstraints**: constrângeri de bază – indică tipul certificatului (certificat de CA sau entitate finală), precum și lungimea maxim admisă pentru lanţul de certificate - **acest câmp este critic** ;

[2] {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (20715); [2] {id-policy}=1; [3] {id-cp}=1;[4] {Class-1}=1

- **CRL DistributionPoints**: punctul de distribuire a Listei certificatelor Revocate – **acest câmp nu este critic**; extensia defineşte adresa din reţea la care se află CRL-ul curent al Autorităţii emitente a certificatului în cauză
- **AuthorityInfoAccessSyntax**: accesul la informaţiile despre Autoritatea de Certificare – **acest câmp nu este critic**; câmpul indică metoda de informare și furnizare a serviciilor de către emitentul certificatului
- **OCSPNoCheck**: dacă este prezentă în cadrul unui certificat al unui responder OCSP, clienţii care primesc răspunsuri OCSP semnate cu o cheie privată asociată certificatului pot avea încredere cu privire la starea acestui certificat pe perioada sa de valabilitate; această extensie **este ne-critică** și este definită de standardul RFC 6960.
- **NetscapeCertType**: această extensie limitează utilizarea certificatului numai la anumite aplicaţii specificate de valoarea extensiei. Dacă nu este prezentă, certificatul poate fi folosit pentru orice aplicaţie cu excepţia aplicaţiilor de ObjectSigning. Extensia **este ne-critică**, iar valoarea să poate fi o combinaţie din următoarele:
  - **SSLClient** (bit 0) – certificatul poate fi folosit pentru autentificarea unui client SSL
  - **SSLServer** (bit 1) – certificatul poate fi folosit pentru autentificarea unui SSL server
  - **S/MIME** (bit 2) – certificatul poate fi folosit de clienţi de mail securizat S/MIME
  - **ObjectSigning** (bit 3) - certificatul poate fi folosit pentru semnarea obiectelor cum ar fi apleturi Java sau plugin–uri
  - **SSL CA** (bit 5) - certificatul poate fi folosit pentru emiterea de certificate utilizate pentru SSL
  - **S/MIME CA** (bit 6) - certificatul poate fi folosit pentru emiterea de certificate utilizate pentru S/MIME
  - **ObjectSigning CA** (bit 7) – certificatul poate fi folosit pentru emiterea de certificate utilizate pentru ObjectSigning
  - Observaţie: pentru valoarea extensiei NetscapeCertType, bitul 4 nu este încă definit fiind rezervat pentru o utilizare viitoare

Certificatele emise de către certSIGN pot conține diferite combinaţii ale extensiilor:

7.1.2.1 Certificatele Autorităţilor de Certificare

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

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.

Certificatele Autorităţilor de certificare pot conține extensiile din Tabelul 7.1.3. și 7.1.5

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=none	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5), cRLSign (bit 6)	critică

Tabelul 7.1.3. Extensiile certificatului certSIGN Root CA

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=0	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5), cRLSign (bit 6)	critică
CRL Distribution Points	http://crl.certsign.ro/root.crl	ne-critică
Certificate Policies	Policies: 1.3.6.1.4.1.25017.1.1.{2,3,4} CPS: http://www.certsign.ro/repository	ne-critică
Authority Info Access	OCSP: http://ocsp.certsign.ro ISSUER: http://crl.certsign.ro/root.crt	ne-critică

Tabelul 7.1.5 Extensiile certificatelor pentru Autoritățile Intermediare (Clasele 2-4) G2

7.1.2.2 Cross-certificarea și certificatele de ne-repudiere

Certificatele pentru cross-certificare și certificatele de ne-repudiere pot conține extensiile specificate în Tabelele 7.1.3., 7.1.14 și 7.1.15.

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint={none,1,2,...}	critică
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1), keyCertSign (bit 5) cRLSign (bit 6)	critică
CRL Distribution Points	URI: http://crl.certSIGN.ro/class4.crl http://crl.certsign.ro/class4g2.crl ldap://ldap.certSIGN.ro/C=RO,O=certSIGN,OU=certSIGN Class 4?certificateRevocationList;binary	ne-critică
Authority Info Access	OCSP: http://ocsp.certSIGN.ro	ne-critică
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.4 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.1.13 Extensiile certificatelor de ne-repudiere

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.

Extension	Value or Value constraint	Extension status
Key Usage	digitalSignature (bit 0), ~~nonRepudiation (bit 1)~~	critică
Extended Key Usage	OCSPSigning	ne-critică
OCSPNoCheck	-	ne-critica
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.{2,3,4}.1 CPS: http://www.certSIGN.ro/repository	ne-critică

Tabelul 7.1.14Extensiile certificatelor de Autoritate de OCSP

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type=CA, Path length constraint=0	Critical
Key Usage	keyCertSign (bit 5) cRLSign (bit 6)	Critical
CRL Distribution Points	URI: http://crl.certsign.ro/root.crl	Non-critical
Authority Info Access	OCSP: http://ocsp.certsign.ro CRT: http://www.certsign.ro/certcrl/root.crt	Non-critical
Certificate Policies	Politicile:1.3.6.1.4.1.25017.1.1.3 CPS: http://www.certSIGN.ro/repository	Non-critical
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	Non-critical

Table 7.1.16. Extensiile certificatului încrucișat pentru certSIGN Web CA

Pe lângă extensiile prezentate mai sus, în certificate se pot introduce la cererea clientului și alte extensii particulare, în condiţii stabilite la momentul contractului.

7.1.3 Identificatorul algoritmului semnăturii electronice

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.
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 Formate de nume

Codificarea numelui
Conținuul câmpurilor de nume trebuie să fie conforme cu cerințele din secțiunea 3.1 precum și cu cerințele ultimei versiuni publicate a CAB Forum BR.
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 CBAF 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 privind numele

Nu se aplică.

7.1.6 Identificatorul de obiect pentru politica de identificare

Table 7.1.2 Identificatori de obiect pentru politica de certificare

7.1.7 Utilizarea extensiei „Policy Constraints"

Nu se aplică.

7.1.8 Sintaxa și semantica calificatorilor de politică

certSIGN emite certificate care conțin un calificator de politică în cadrul extensiei Politicile certificatului. Această extensie conține un calificator CPS care trimite către CPP.

7.1.9 Semantica de procesare pentru extensia critică „Certificate Policies"

Nu se aplică.

7.2 Profilul CRL

Lista de certificate Revocate (CRL) constă din trei câmpuri. Primul câmp (**tbscertList**) conține informaţii despre certificatele revocate, al doilea și al treilea câmp – **signatureAlgorithm** și **signatureValue** conţin informaţii despre identificatorul algoritmului folosit pentru semnarea listei și semnatura electronica a Autorităţii de Certificare.

Câmpul **tbscertList** este o secvenţă de câmpuri obligatorii și opţionale. Câmpurile obligatorii identifică emitentul CRL-ului în timp ce câmpurile opţionale conţin informaţii despre certificatele revocate și extensiile CRL-ului.

Conţinutul câmpurilor obligatorii și opţionale dintr-un CRL sunt următoarele:

- **Version**: versiunea formatului de CRL,
- **signature**: identificatorul algoritmului folosit de Autoritatea de Certificare pentru a semna CRL-ul; autorităţile certSIGN semnează CRL-urile folosind algoritmul **sha256WithRSAEncryption**,
- **Issuer**: numele Autorităţii de Certificare care a emis CRL-ul; fiecare autoritate a certSIGN emite propria sa Listă de certificate Revocate; acest lucru se aplică următoarelor autorități: **certSIGN SSL DV CA Class 3 G2**
- **ThisUpdate**: data publicării CRL-ului,
- **NextUpdate**: date la care se va publica următorul CRL; dacă câmpul este prezent, valoarea sa descrie data maximă până la care se va face actualizarea CRL-ului,
- **Revokedcertificates**: lista certificatelor revocate (câmpul este gol în cazul în care nu a fost revocat nici un certificat); informaţia constă din trei sub-câmpuri:

  usercertificates – numărul serial al certificatului revocat;

  revocationDate – data revocării certificatului;

  crlEntryExtensions – conține informaţii suplimentarea despre certificatele revocate - opţional.

- **crlExtensions**: informaţii suplimentare despre Lista de certificate Revocate (câmp opţional). Dintre extensiile posibile, cele mai importante sunt următoarele: **AuthorityKeyIdentifier** (vezi și Capitolul 7.1.2) care permite identificarea cheii publice corespunzătoare cheii private folosită pentru semnarea listei și **cRLNumber**, care conține un număr serial incrementat monoton al listei emisă de Autoritatea de Certificare (prin intermediul acestei extensii, Beneficiarul are posibilitatea de a determine dacă a fost publicat un nou CRL).

7.2.1 Numerele de versiune

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

7.2.2 CRL și extensiile 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.
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.
Rolul și semnificaţia extensiilor este aceleași ca în cazul extensiilor de certificat (vezi Capitolul 7.1.2). Extensiile dintr-o intrare CRL (**crlEntryExtensions**) acceptate de certSIGN- conţin următoarele câmpuri:

ReasonCode: codul motivului revocării certificatului. **Acest câmp nu este critic** și permite determinarea motivului revocării unui certificat. Sunt permise următoarele motive de revocare pentru certificatele care NU sunt de tip SSL/TLS:

- **unspecified** – nespecificat;
- **keyCompromise** – compromiterea cheii;
- **cACompromise** – compromiterea cheii Autorităţii de Certificare;
- **affiliationChanged** – modificarea datelor Beneficiarului;
- **superseded** – înnoirea certificatului;
- **cessationOfOperation** – sistarea folosirii certificatului;
- **privilegeWithdrawn** – retragerea drepturilor
- **certificateHold** – suspendarea certificatului;
- **removeFromCRL** – eliminarea certificatului din CRL.

Motivele ReasonCode **unspecified** – nespecificat, precum **certificateHold** – suspendarea certificatului NU sunt permise pentru revocarea certificatelor emise de certSIGN Enterprise CA Class 3 G2.
Dacă un răspuns CRL este pentru un Certificat de Root CA sau de CA Intermediar, inclusiv pentru Cross Certificate, extensia CRL entry ReasonCode este întotdeauna prezentă, cu o valoare permisă.
Pentru certificatele de tip SSL/TLS motivele de revocare permise, cu cod in **CRL Reason**:

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].

7.3 Profilul OCSP

Protocolul de verificare on-line a stării certificatelor (OCSP) permite determinarea stării unui certificat.

Serviciul OCSP este oferit de certSIGN în numele tuturor Autorităţilor de Certificare afiliate. Serverul OCSP, care emite confirmări ale stării certificatelor, foloseşte o pereche specială de chei, generată exclusiv pentru acest scop.

Certificatul serverului OCSP trebuie să conţină extensia extKeyUsage, descrisă în RFC 3280. Această extensie trebuie declarată ca fiind ne-critică și semnifică faptul că o Autoritate de Certificare care emite certificatul pentru serverului OCSP confirmă prin semnatura sa delegarea autorizării de a emite confirmări ale stării certificatelor (aparţinând Abonaților acestei autorități).

De asemenea, certificatul serverului OCSP conține extensia OCSPNoCheck, descrisă de RFC 6960. Această extensie trebuie declarată ca fiind ne-critică și semnifică faptul că un client de OCSP care primeşte un răspuns semnat cu cheia privată asociată acestui certificat va putea avea încredere în starea certificatului serverului OCSP, nefiind necesară verificarea stării de revocare a acestuia.

[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*

Entitatea care primeşte o confirmare emisă de serverul OCSP trebuie să suporte formatul standard de răspuns având identificatorul **id-pkix-ocsp-basic** .

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

- GOOD – indică faptul că certificatul este în stare validă

- REVOKED – indică faptul că certificatul a fost emis și a fost revocat sau certificatul nu a fost emis conform RFC 6960

- UNKNOWN – indică faptul că nu există suficiente informaţii pentru determinarea stării certificatului respectiv

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

7.3.1 Numărul versiunilor

Serverul OCSP care operează în cadrul certSIGN emite confirmări de stare a certificatului în conformitate cu RFC 6960. Singura valoare admisibilă a numărului de versiune este 0 (este echivalentul versiunii v1).

7.3.2 Extensii OCSP

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

Nonce – Obligarea unei solicitări și a unui răspuns pentru a preveni atacurile de replay. **Nonce** este inclus în **requestExtension** al **OCSPRequest** și repetat în câmpul **responseExtension** al **OCSPResponse**.
Dacă un răspuns OCSP este pentru revocarea unui certificat de CA ROOT sau de CA Intermediar, inclusiv Cross-Certificate, iar certificatul a fost revocat, atunci câmpul **revocationReason** din cadrul **RevokedInfo** al **CertStatus** este prezent, și are o valoare permisă pentru CRLuri, conform cu secțiunea 7.2.2 de mai sus.
Pentru certificatele de utilizator final solicitate pentru a fi revocate, această extensie NU este utilizată.