Anexa Profile la

Codul de Practici și Proceduri

certSIGN

SSL EV CA Clasa 3 G2

pentru certificate SSL EV

Versiunea 1.17

Data: 31 Iulie 2023

Notă
importantă

Adresa: Bulevardul Tudor Vladimirescu nr. 29 A,
AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901
Fax: 004-021-31.19.905

Web:www.certsign.ro

Istoric document

Versiune	Data Efectivă	Motiv	Persoana care a făcut schimbarea
1.17	31 Iulie 2023	Prima versiune	Manager Politici PKI

Acest document a fost aprobat de

Versiune	Nume	Data
1.17	Comitetul de Management al Politicilor si Procedurilor	Iulie 2023

Contents

7 CERTIFICAT, CRL ȘI PROFIL OCSP 3

7.1 PROFILUL CERTIFICATULUI 3

7.1.1 Număr de versiune 4

7.1.2 Extensii de certificate 4

7.1.3 Identificatori de algoritm obiect 8

7.1.4 Forme de nume 8

7.1.5 Constrângeri de nume 9

7.1.6 Identificator de obiect al politicii de certificat 9

7.1.7 Utilizarea extensiei de constrângeri de politică 9

7.1.8 Sintaxa și semantica calificativelor de politici 9

7.1.9 Prelucrarea semanticii pentru extensia critică de politici de certificat 9

7.2 PROFIL CRL 9

7.2.1 Numere de versiune 10

7.2.2 Extensii de intrare CRL și CRL 10

7.3 PROFIL OCSP 11

7.3.1 Numere de versiune 12

7.3.2 Extensii OCSP 12

7 Certificat, CRL și profil 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, au aplicat extensii standard și private utilizate de CERTSIGN.

7.1 Profilul certificatului

Profilul câmpurilor de bază pentru certificatul certSIGN SSL EV CA Clasa 3 G2 descris în tabelul 7.1.

Field name	Value or value's constraint	
Version	3	
Serial Number	2006051670031857926 01acb75e127	
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 09:46:55 2018 GMT	
Not after (validity period end date)	Jan 30 09:46:55 2028 GMT	
Subject (Distinguished Name)	Common Name (CN)	certSIGN SSL EV CA Class 3 G2
	Organisation Unit (OU) =	certSIGN SSL EV 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 EV CA Clasa 3 G2

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

Field name	Value or value's constraint
Version	Version 3

Field name	Value or value's constraint	
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 EV CA Class 3 G2
	Organisational Unit =	certSIGN SSL EV 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, may contain fields 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 emise de certSIGN SSL EV CA Clasa 3 G2

7.1.1 Număr de versiune

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

7.1.2 Extensii de certificate

Extensiile de certificate pentru certSIGN SSL EV 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)	Non-critical

Extension	Value or Value constraint	Extension status
	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	
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	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.25017.1.1.6 [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 EV CA Clasa 3 G2

Certificatul SSL EV conține extensii 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)	Non-critical

Extension	Value or Value constraint	Extension status
	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	
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)	Critical
Authority Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	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=1.3.6.1.4.1.25017.1.1.6.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=2.23.140.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical

Extension	Value or Value constraint	Extension status
CRL Distribution Points	http://crl.certsign.ro/certsign-sslev.crl	Non-critical
Subject Alternative Name	This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for SSL EV.	Non-critical
Enhanced 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
cabfOrganization Identifier	cabfOrganizationIdentifier: 2.23.140.3.1 {joint-iso-itu-t(2)international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) } Acest câmp optional, daca exista, trebuie să conțină o referință de înregistrare pentru o entitate juridică alocată în conformitate cu schema de înregistrare identificată, după cum este specificat în Secțiunea 9.8.2 din EV Guidelines.	Non-critical

Tabelul 7.4. SSL EV extensii de certificate

Certificatul OCSP conține extensii descrise în tabelul 7.5.

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/certsign-sslev.crt	Non-critical

Extension	Value or Value constraint	Extension status
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1)	Critical
Authority Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	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
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.1.1.6.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://crl.certsign.ro/certsign-sslev.crl	Non-critical
Subject Alternative Name	Other Name: Principal Name=office@certsign.ro RFC822 Name=office@certsign.ro	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

Câmpul signatureAlgorithm conține un identificator de algoritm criptografic utilizat pentru semnătura electronică creat de o autoritate de certificare pe certificat. În cazul CERTSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

Pentru algoritmul cheii publice se folosește Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA

Parametrii sunt prezenți, ca un NULL explicit.

7.1.4 Forme de nume

Conținutul câmpurilor trebuie să îndeplinească cerințele din secțiunea 3.1 și ghidurile ultimei versiuni publicate ale EV Forum CAB.

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.

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 EV CA Clasa 3 G2 sunt descrise în Tabelul 7.6 și Tabelul 7.7.

Certification Policy Name	Policy identifier
certSIGN SSL EV CA Class 3 G2	{certSIGN} .{id-policy}(1). {id-cp}(1).{id-EV-CA}(6) . *subpolicy ID=1.3.6.1.4.1.25017.1.1.6. subpolicy ID* See below table for *subpolicyID* values. *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) }(2.23.140.1.1)*

Tabelul 7.6. Identificatorii politicilor și numele acestora

CA Level	OID
certSIGN SSL EV CA Class 3 G2 1.3.6.1.4.1.25017.1.1.6	*SSL EV certificate .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
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)

Field name	Value or value's constraint	
Issuer	Common Name (CN)	certSIGN SSL EV CA Class 3 G2
	Organisational Unit (OU)=	certSIGN SSL EV 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 EV CA Clasa 3 G2

7.2.1 Numere de versiune

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

7.2.2 Extensii de intrare CRL și CRL

Extensiile CRL pentru certSIGN SSL EV CA Clasa 3 G2 sunt descrise în Tabelul 7.9.

Extension	Value or Value constraint	Extension status
Authority Key Identifier	36 3b a2 9e 25 87 2a 0f fd 9a 4a 3c 27 da cb a7 79 c3 0c 7f	Non-critical
CRL Number	monotonically increasing sequence number	Non-critical
crlEntryExtensions	reason for revocation	Non-critical
CRL Reason	Revocation reason code	Non- critical

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

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 organizației sau alte informații organizaționale din certificat s-au modificat.

4. Superseded (RFC 5280 CRLReason # 4)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "superseded" atunci când solicită un nou certificat pentru a înlocui certificatul existent.
5. CessationOfOperation (RFC 5280 CRLReason # 5)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "cessationOfOperation" atunci când nu mai deține toate numele de domeniu din certificat sau când nu va mai utiliza certificatul, deoarece își întrerupe site-ul web.
6. privilegeWithdrawn (RFC 5280 CRLReason #9)[1]
   - 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.

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 Intermediar și ROOT CA, generată exclusiv în acest scop.

Certificatul de server OCSP trebuie să conțină extensia extKeyUsage, descrisă în RFC 5280.

Această extensie ar trebui 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 trebuie 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

[1] *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*

- UNKNOWN - 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** din **OCSPRequest** și repetat în câmpul **responseExtension** din **OCSPResponse**.