Annex Profiles for Certification Practice Statement certSIGN SSL DV CA Class 3 G2 for SSL DV certificates

Version 1.22

Date: 15 January 2026

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,
AFI Tech Park 1, Bucharest, Romania
Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date[1]	Reason	The person who made the change
1.18	July 2023	First version	PKI Policies Manager
1.19	Jan.2024	Annual review	PKI Policies Manager
1.20	Jan.2025	Annual review	PKI Policies Manager
1.21	Apr.2025	Update footer	PKI Policies Manager
1.22	15 Jan.2026	Annual review	PKI Policies Manager

This document was approved by:

Version	Name	Date
1.18	Policies and Procedures Management Body	July 2023
1.19	Policies and Procedures Management Body	Jan.2024
1.20	Policies and Procedures Management Body	Jan.2025
1.21	Policies and Procedures Management Body	Apr.2025
1.22	Policies and Procedures Management Body	Jan.2026

Content

[1] *Effective date is the last day of the month*

7 Certificate, CRL and OCSP profile

Certificate profiles and Certificate Revocation List (CRL) profile comply with the format described in ITU-T X.509 v.3 standard, while the profile of OCSP complies with the requirements of RFC 6960. Information stated below describes the meaning of respective certificate fields, CRL and OCSP, applied standard and private extensions used by CERTSIGN.

7.1 Certificate profile

certSIGN CA meets the technical requirements set forth in CABF BR Section 2.2 - Publication of Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.
SerialNumber field is a non-sequential number greater than zero (0) and less than 2^{159} containing at least 64 bits of output from a CSPRNG.
All objects signed by a certSIGN CA Private Key conform to the CABF BR #7.1.3.2, RSA or ECDSA requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.
The SubjectPublicKeyInfo field indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier, with an explicit NULL parameter.
The AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.
For ECDSA, the identifiers and encodings specified in #7.1.3.2 from CABF BR will be used.

TLS Subordinate CA Certificate Profile
All subject names are encoded as specified in Section 7.1.4 and contain the AttributeTypes following #7.1.2.10.2 "CA Certificate Naming" from CABF BR.

Profile of basic fields for certSIGN SSL DV CA Class 3 G2 certificate is described in Table 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	Jan 30 09:44:44 2018 GMT	
Not after	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)	

Table 7.1. Profile of the basic fields for certSIGN SSL DV CA Class 3 G2

Subscriber (Server) Certificate Profile

The notBefore field has a value within 48 hours of the certificate signing operation.
All subject names are encoded as specified in Section 7.1.4 and contain the AttributeTypes following #7.1.2.7.2 "Domain Validated" from CABF BR.
Subscriber Certificate Common Name Attribute contain exactly one entry that is one of the values contained in the Certificate's subjectAltName extension, encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name will be encoded as LDH Labels, and P-Labels will NOT be converted to their Unicode representation.

Profile of basic fields for end-user DV certificates issued by certSIGN SSL DV CA Class 3 G2 is described in Table 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 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.	

Table 7.2. Profile of the basic fields of end-user DV certificates issued by certSIGN SSL DV CA Class 3 G2

Precertificate Profile
A Precertificate appears structurally identical to a end-user DV Certificate, with the exception of a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3, and is created after a CA has decided to issue a Certificate, but prior to the actual signing of the Certificate.
The basic fields of the precertificate:

- **version** Encoded value MUST be byte-for-byte identical to the version field of the Certificate
- **serialNumber** Encoded value MUST be byte-for-byte identical to the serialNumber field of the Certificate (as an exception to RFC 5280, Section 4.1.2.2)
- **signature** Encoded value MUST be byte-for-byte identical to the signature field of the Certificate
- **issuer** Encoded value MUST be byte-for-byte identical to the issuer field of the Certificate
- **validity** Encoded value MUST be byte-for-byte identical to the validity field of the Certificate
- **subject** Encoded value MUST be byte-for-byte identical to the subject field of the Certificate
- **subjectPublicKeyInfo** Encoded value MUST be byte-for-byte identical to the subjectPublicKeyInfo field of the Certificate
- **issuerUniqueID** Encoded value MUST be byte-for-byte identical to the issuerUniqueID field of the Certificate, or omitted if omitted in the Certificate
- **subjectUniqueID** Encoded value MUST be byte-for-byte identical to the subjectUniqueID field of the Certificate, or omitted if omitted in the Certificate

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.	

OCSP Responder Certificate Profile

The Issuing CA of the Responder is the same as the Issuing CA for the Certificates it provides responses for.

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 Version number(s)

All certificates issued by CERTSIGN are X.509 version 3.

7.1.2 Certificate extensions

The certificates profiles extensions are according to CABF BR # 7.1.2 "Certificate Content and Extensions".

TLS Subordinate CA Certificate Profile Extensions

The ***AuthorityInfoAccess*** contain one or more AccessDescriptions. Each AccessDescription only contains a permitted accessMethod, and each accessLocation is encoded as the specified GeneralName type.

Authority Key Identifier extension have only the ***keyIdentifier*** field, identical to the subjectKeyIdentifier field of the Issuing CA.

CA Certificate ***Basic Constraints***: cA set TRUE; pathLenConstraint set to 0 or NULL.

Certificate Policies extension contains at least one PolicyInformation and it contain exactly one Reserved Certificate Policy Identifier – for CA certificates issued after 2023.

The ***CRL Distribution Points*** extension contains at least one DistributionPoint, of type uniformResourceIdentifier, and the scheme of each is "http". The first GeneralName contains the HTTP URL of the Issuing CA's CRL service for the CA certificate.

certSIGN CA generates a ***subjectKeyIdentifier*** that is unique within the scope of all Certificates it has issued for each unique public key.

For CA certificates issued after 2023 - the CA Certificate ***Extended Key Usage*** contains id-kp-serverAuth key, and optionally id-kp-clientAuth.

Certificate extensions for certSIGN SSL DV CA Class 3 G2 are described in Table 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

Table 7.3. Extensions of certSIGN SSL DV CA Class 3 G2 certificate

Subscriber (Server) Certificate Profile Extensions

The ***AuthorityInfoAccess*** contain one or more AccessDescriptions. Each AccessDescription only contains a permitted accessMethod, and each accessLocation is encoded as the specified GeneralName type.

Authority Key Identifier extension have only the ***keyIdentifier*** field, identical to the subjectKeyIdentifier field of the Issuing CA.

Certificate Policies extension contains at least one PolicyInformation and it contain exactly one Reserved Certificate ***Policy Identifier***:

*{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), HTTP or HTTPS URL for the Issuing CA's Certification Practice Statement.

The end-user DV Certificate ***Extended Key Usage*** contains id-kp-serverAuth key, and optionally id-kp-clientAuth.

The ***Subject Alternative Name*** is present and contains at least one dNSName. dNSName contains either a Fully-Qualified Domain Name or Wildcard Domain Name that the CA has validated in accordance with CABF BR Section 3.2.2.4. Wildcard Domain Names are validated for consistency with CABF BR Section 3.2.2.6. The dNSName entry does not contain an Internal Name. The Fully-Qualified Domain Name or the FQDN portion of the

Wildcard Domain Name contained in the entry is composed entirely of P-Labels or Non-Reserved LDH Labels joined together by a U+002E FULL STOP (".") character. The zero-length Domain Label representing the root zone of the Internet Domain Name System is NOT included.
Key Usage values: digitalSignature and keyEncipherment.
The ***CRL Distribution Points*** extension contains at least one DistributionPoint, of type uniformResourceIdentifier, and the scheme of each is "http". The first GeneralName contains the HTTP URL of the Issuing CA's CRL service for the CA certificate.

End User DV SSL certificate contains extensions described in Table 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 contains at least one entry. Each entry is a DNS Name containing the Fully-Qualified Domain Name 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)	

Table 7.4. End-User DV certificate extensions

Precertificate Profile Extensions

The Precertificate contains the Precertificate Poison extension (OID:1.3.6.1.4.1.11129.2.4.3). This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962, Section 3.1.

OCSP Responder Certificate Profile Extensions

Authority Key Identifier extension have only the ***keyIdentifier*** field, identical to the subjectKeyIdentifier field of the Issuing CA.

OCSP Responder Extended Key Usage is only OCSP Signing (1.3.6.1.5.5.7.3.9).certSIGN CA includes the ***id-pkix-ocsp-nocheck*** extension (OID: 1.3.6.1.5.5.7.48.1.5).

This extension has an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6960, Section 4.2.2.2.1.

OCSP Responder ***Key Usage*** is only digitalSignature.

subjectAltName, authorityInformationAccess, certificatePolicies, crlDistributionPoints are not set as extensions for OCSP certificates issued after 2023.

OCSP certificate contains extensions described in Table 7.5.

Extension	Value or Value constraint	Extension status
Key Usage	digitalSignature (bit 0), nonRepudiation (bit 1) [2]	Critical
Authority Key Identifier	f5dcbbfb891eca7881746cb64a6c254d54817e06	Non-critical
Subject Key Identifier	3c767c4a3c2d6c5a82c02d62f92e1789e555f0b6	Non-critical
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Non-critical
OCSPNoCheck		Non-critical

Table 7.5. OCSP certificate extensions

7.1.3 Algorithm object identifiers

SubjectPublicKeyInfo

The SubjectPublicKeyInfo field indicate an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier, with an explicit NULL parameter.

The AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500.

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

For ECDSA, the identifiers and encodings specified in #7.1.3.1.2 from CABF BR will be used.

Signature AlgorithmIdentifier
All objects signed by a certSIGN CA Private Key conform to the CABF BR #7.1.3.2, RSA or ECDSA requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures. In the case of certSIGN, the algorithm used is sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Name forms

Name Encoding
The contents of the fields in DV certificates must meet the requirements in section 3.1 and the latest published version of CAB Forum Baseline Requirements Certificate Policy.
Issuer Name for all possible certification paths is byte-for-byte identical with Subject Name of the Issuer certificate. Subject attributes do not contain only metadata such as '.', '-', and ' ' (i.e. space) to indicate that the value is absent, incomplete, or not applicable.
For every valid Certification Path (as defined by RFC 5280, Section 6):
• For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
• For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

Subject Attribute Encoding
The attributes in the Certificate subject field will be encoded and positioned according to Table 77: "*Encoding and Order Requirements for Selected Attributes*" from CBAF BR section 7.1.4.2 Subject Attribute Encoding.

Subscriber Certificate Common Name Attribute
This attribute contains exactly one entry that is one of the values contained in the Certificate's subjectAltName extension.
If the value is a Fully-Qualified Domain Name or Wildcard Domain Name, then the value is encoded as a character-for-character copy of the dNSName entry value from the subjectAltName extension. Specifically, all Domain Labels of the Fully-Qualified Domain Name or FQDN portion of the Wildcard Domain Name must be encoded as LDH Labels, and P-Labels will NOT be converted to their Unicode representation.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

Certificates policy object identifiers used at certSIGN SSL DV CA Class 3 G2 level are described in Table 7.6 and Table 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.

Table 7.6. Policies identifiers and their names for certSIGN SSL DV CA Class 3 G2 certificates

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***

Table 7.7 Certificate policy object identifiers

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

certSIGN issue certificates with a policy qualifier within the Certificate Policies extension. This extension contains a CPS pointer qualifier that points to the CPS.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

certSIGN CA uses full and complete CRL, that is a CRL whose scope includes all Certificates issued by the CA.

nextUpdate field indicates the date by which the next CRL will be issued. For CRLs covering Subscriber Certificates, at most 10 days after the ***thisUpdate***. For other CRLs, at most 12 months after the ***thisUpdate***.

revokedCertificates field is present if the CA has issued a Certificate that has been revoked and the corresponding entry has yet to appear on at least one regularly scheduled CRL beyond the revoked Certificate's validity period. The CA will remove an entry for a corresponding Certificate after it has appeared on at least one regularly scheduled CRL beyond the revoked Certificate's validity period.

CRL profile is described in Table 7.8.

Field name	Value or value's constraint
Version	V2

Field name	Value or value's constraint	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Common Name (CN) =	certSIGN SSL DV CA Class 3 G2
	Organisational Unit (CN) =	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	

Table 7.8 CRL profile for certSIGN SSL DV CA Class 3 G2

7.2.1 Version numbers (s)

All CRLs issued by CERTSIGN are X.509 version 2.

7.2.2 CRL and CRL entry extensions

CRLNumber extension contains an INTEGER greater than or equal to zero (0) and less than 2^{159}, and convey a strictly increasing sequence.

CRL extensions for certSIGN SSL DV CA Class 3 G2 are described in Table 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

Table 7.9. CRL extensions for certSIGN SSL DV CA Class 3 G2

serialNumber is byte-for-byte identical to the ***serialNumber*** contained in the revoked Certificate.

revocationDate is the date and time revocation occurred.
The CA updates the revocation date in a CRL entry when it is determined that the private key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate. Backdating the revocationDate field is an exception to best practice described in RFC 5280 (Section 5.3.2); the revocationDate field support TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised.

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*

Table 7.10. revokedCertificates Component for certSIGN SSL DV CA Class 3 G2

CRL entry extensions (***crlEntryExtensions***) supported by certSIGN contain the following fields: **ReasonCode**: code of the reason for revocation. This field is non-critical, allowing determination of the certificate revocation reason. The following reasons of certificate revocation are allowed:

1. No reason provided (RFC 5280 CRLReason #0)
   - When the reason codes do not apply to the revocation request, the subscriber MUST NOT provide a reason code. If the reason for revocation is unspecified, the CA will omit reasonCode entry extension.
2. keyCompromise (RFC 5280 CRLReason #1)
   - The certificate subscriber MUST choose the "keyCompromise" revocation reason when they have reason to believe that the private key of their certificate has been compromised, e.g. an unauthorized person has had access to the private key of their certificate.
3. affiliationChanged (RFC 5280 CRLReason #3)
   - The certificate subscriber SHOULD choose the "affiliationChanged" revocation reason when their Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
4. superseded (RFC 5280 CRLReason #4)
   - The certificate subscriber SHOULD choose the "superseded" revocation reason when the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the Baseline Requirements or the CA's CPS..
5. cessationOfOperation (RFC 5280 CRLReason #5)
   - The certificate subscriber SHOULD choose the "cessationOfOperation" revocation reason when the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate. .
6. privilegeWithdrawn (RFC 5280 CRLReason #9)[3]
   - The CRLReason privilegeWithdrawn is intended to be used when there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the certificate subscriber provided misleading information in their certificate request or has not upheld their material obligations under the subscriber agreement or terms of use.

The Subscriber Agreement inform Subscribers about the revocation reason options listed above and provide explanation about when to choose each option. Revocation requests templates, that the CA provides to the Subscriber, allow for these options to be easily

[3] *The privilegeWithdrawn reasonCode does not need to be made available to the certificate subscriber as a revocation reason option, because the use of this reasonCode is determined by the CA operator and not the subscriber.*

specified when the Subscriber requests revocation of their Certificate, with the default value being that no revocation reason is provided (i.e. the default corresponds to the CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL).

7.3 OCSP profile

The protocol of on-line certificate status verification (OCSP) allows certificate status evaluation.

OCSP service is provided by CERTSIGN on behalf of all affiliated Certification Authorities. OCSP server, which issues certificate status confirmations, employs a special key pair for each Intermediate CA and Root CA, generated exclusively for this purpose.

OCSP server certificate contains the extension ***extKeyUsage***, described in RFC 5280.

This extension is set as non-critical, and means that a Certification Authority issuing the certificate to the OCSP server confirms with its signature delegation of the authorization to issue certificate status conformation (of this authority's Subscribers).

As well, OCSP server certificate contains the ***OCSPNoCheck*** extension, described by RFC 6960. This extension is declared non-critical which means that an OCSP client receives a response signed with the private key associated to this certificate can trust the OCSP server certificate status, without being necessary to check its revocation status.

The entity receiving a confirmation issued by the OCSP server must support the standard response format with **id-pkix-ocsp-basic** identifier.

Information about certificate status is included in **certStatus** field of **SingleResponse** structure. This may have one of the following three main values:

- GOOD – indicates the valid status of certificate

- REVOKED – indicates that the certificate was issued and revoked or the certificate was not issued in accordance with the RFC 6960

- UNKNOWN – indicates that there is not enough information to determine the certificate status

When the OCSP answer contains an error code (message), the answer is not digitally signed (RCF 6960).

7.3.1 Version numbers (s)

OCSP server operating within CERTSIGN issues certificate status confirmations in accordance with the RFC 6960. The only allowable value of the version number is 0 (it is an equivalent of v1 version).

7.3.2 OCSP extensions

In compliance with RFC 6960, CERTSIGN OCSP server accepts the following extension:

Nonce – binding a request and a response to prevent reply attacks. **Nonce** is included in **requestExtension** of the **OCSPRequest** and repeated in the field **responseExtension** of the **OCSPResponse**.