

## Formular -Conținutul și structura certificatului calificat

Domeniu	Semnătura electronică	Cod domeniu	SMEL
Titlu document	CONȚINUTUL ȘI STRUCTURA CERTIFICATULUI CALIFICAT		Cod document 03
			Pag 2
Date despre FSC			
Numele Furnizorului de Servicii de Certificare			
Adresa * Țara	Oraș	Sector	Strada nr
	bloc	etaj	apt. Cod poștal
	Tel	Fax	Pagina Web E-mail
Cetățenie / Naționalitate			
Domeniu	Semnătura electronică	Cod domeniu	SMEL
Titlu document	CONȚINUTUL ȘI STRUCTURA CERTIFICATULUI CALIFICAT		Cod document 03
			Pag 2
Numele și prenumele			
Pseudonimul			
Adresa	Tara de rezidență	Județ/Sector	
	Oraș	Strada	Nr.
	Bloc	Scara	Apart.
	Cod poștal	Telefon	Fax
	E-mail	Pagina Web	
Alte informații pe care clientul le dorește a fi cuprinse în certificat			
Tip certificat	CERTIFICAT CALIFICAT		
Cheia publică			
Codul personal de identificare al semnatarului			
Cod de identificare al certificatului			
Extensiile semnăturii (vezi Anexa 4 din Normele metodologice privind aplicarea semnăturii electronice)			
Perioada de valabilitate a certificatului			
Informații privind limitele utilizării certificatului			
Domeniu	Semnătura electronică	Cod domeniu	SMEL
Titlu document	EXTENSIILE CERTIFICATELOR PENTRU SEMNĂTURĂ ELECTRONICĂ		Cod document 04
			Pag 2
Extensia	Utilizat de	Utilizare	Critic
<b>A. Informații cu privire la chei și politica de certificare</b>			
AuthorityKeyIdentifier	Identificator pentru cheia publică a autorității		Toate
Identifică cheia publică corespunzătoare cheii private utilizată de Furnizorul de Certificare pentru a semna acest certificat	Nu		
KeyIdentifier	Identificator al cheii publice		Toate
Identificator unic, în funcție de algoritmul utilizat	Nu		
AuthorityCertIssuer	Numele emitentului certificatului		Toate
Identifică autoritatea de emisie a certificatului; împreună cu numărul seriei, alternativă la identificatorul cheii	Nu		

AuthorityCertSerialNumber	Nr. seriei certificatului	Toate	Utilizat cu Numele emitentului certificatului	Nu
SubjectKeyIdentifier	Identificatorul cheii subiectului	Toate	Identifică chei diferite pentru același subiect	Nu
KeyUsage	Folosirea cheii (exemplu, semnătura digitală, key agreement...)	Toate	Definește scopuri specifice pentru utilizarea cheii (de Opțională	
PrivateKeyUsagePeriod	Perioada de utilizare a cheii private		Toate	
	Numai pentru cheile de semnătură digitală. Semnăturile pe documente date în afara perioadei sunt invalide Opțională			
CertificatePolicies	Politici de certificare		Toate	
	Identificatori și calificatori ce identifică și califică politicile de certificare ce se aplică unui certificat			Opțională
PolicyIdentifiers	Identificatori de politici de certificare		Toate	
	OID = obiectul de identificare a unei politici			Opțională
PolicyQualifiers	Atributele politicii de certificare		Toate	
	Mai multe informații privind politicile de certificare			Opțională
PolicyMappings	Suprapunerea de politici		AC	
	Indică politici echivalente			Opțională
<b>B. Atribute certificat și FSC</b>				
SubjectAltName	Numele alternativ al subiectului (numele RFC822, adresa X400, adresa IP...)	Toate	Utilizată pentru a lista numele alternative (de exemplu Opțională	
IssuerAltName	Numele alternativ al emitentului	Toate	Listează numele alternative	Opțională
SubjectDirectoryAttributes	Toate		Listează orice atribut dorit (de exemplu supported algorithms	Opțională
<b>C. Constrângeri ale căii de certificare</b>				
BasicConstraints	Constrângeri de bază		Toate	
	Constrângeri privind rolul subiectului și lungimea căii DA			
CA	Autoritatea de Certificare		Toate	
	Lungimea căii este semnificativă numai dacă valoarea lui cA - Adevărat DA			
PathLenConstraint	Constrângeri privind lungimea căii de certificare		AC	
	Numărul AC care sunt permise în calea de certificare; 0 indică faptul că AC poate să emită certificate numai către entitatea finală DA			
NameConstraints	Constrângeri privind numele		AC	
	Limitează certificarea AC consecutive referitor la următorii doi parametri: PermittedSubtrees și ExcludedSubtrees Opțională			
PermittedSubtrees	Subarbori permisi			
	Numele din afara subarborilor indicați nu sunt permise Opțională			