

EFOS End Entity Function Certificates

Field	Value	Comments	Source
Version	V3 (2)		CA
Serial Number	Unique number		CA
Issuer Signature Algorithm	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Issuer Distinguished Name	Unique X.500 CA DN. CN = Swedish Public Sector Function CA v1 O = Swedish Social Insurance Agency C = SE		CA
Validity Period	Up to 24 months expressed in UTC format		Certificate Management Tool based on CA templates
Subject Distinguished Name			
SerialNumber	Subject:serialNumber (2.5.4.5)	This field MUST contain the Subject's unique ID. 1. If generated by Efos it will have following format: EFOS16NNNNNNNNNN-NNNNNN. It's alphanumerical and 23 characters long. It consists of an organization unique prefix and a suffix unique to each function in that organization. The two parts are separated by a hyphen	Certificate Management Tool 1: EFOS16<Org. Nr>-<counter>
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain an entity owned by the requesting organization This field MUST contain one of the following: - Client Name - Function Email Address - FQDN of function	Certificate Management Tool: Manual, but matched against a ruleset
OrganizationUnit	subject:orgUnit (2.5.4.11)	This field MUST contain the Subject's full legal organization number as listed in the official records in the following format: NNNNNNNNNN	Certificate Management Tool: Companies Registration Office, Central Bureau of Statistics and WHOIS
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization	Certificate Management Tool:

		name as listed in the official records.	Companies Registration Office, Central Bureau of Statistics
Locality	subject:localityName (2.5.4.7)	This field MUST contain the locality/municipality of the headoffice for the Subject's organization as listed in the official records	Certificate Management Tool: Companies Registration Office, Central Bureau of Statistics
Email	Subject:emailAddress (1.2.840.113549.1.9.1)	This field CAN contain the email address of the Subject	Certificate Management Tool: 1: Manual
Country	subject:countryName (2.5.4.6)	This field MUST contain the country code for the Subject's organization as listed in the official records. In ISO3166 format	Certificate Management Tool: Companies Registration Office, Central Bureau of Statistics
Subject Public Key Information	2048-4096-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)	Min 2048-bit – Max 4096-bit	CA
Issuer's Signature	sha256 WithRSAEncryption (1.2.840.113549.1.1.11)		CA
Extension	Value		
Authority Key Identifier	c=no; Octet String – Same as Issuer's subject key identifier	Contains 20 byte SHA-2 hash of the CA Public Key	CA
Subject Key Identifier	c=no; Octet String – Calculated by CA from public key in PKCS#10	Contains 20 byte SHA-2 hash of the subjectPublicKey in this certificate	CA
Certificate Policies	c=no; [1]Certificate Policy: Policy Identifier= 1.2.752.146.240.2 https:// repository.efos.se	OID: Function ID CA v1 = 1.2.752.146.240.2	Certificate Management Tool based on CA templates
Key Usage	c=yes; Digital Signature, Key Encipherment (a0) OR nonRepudiation (40)	This field MUST contain Digital Signature, Key Encipherment (a0) OR nonRepudiation (40)	Certificate Management Tool based on CA templates
Extended Key Usage	c=no; Client Authentication (1.3.6.1.5.5.7.3.2) AND Server Authentication (1.3.6.1.5.5.7.3.1) OR Secure E-Mail (1.3.6.1.5.5.7.3.4) OR If Key Usage=nonRepudiation	This field MUST contain Client Authentication AND Server Authentication OR Secure E-Mail] OR If Key Usage=nonRepudiation Document Signing	Certificate Management Tool based on CA templates

	Document Signing (1.3.6.1.4.1.311.10.3.12)		
Subject Alternative Name	<p>c=no; DNS = FQDN of Function (e.g., domain.com)</p> <p>OR</p> <p>RFC822Name = mailbox@domain.suffix</p> <p>OR</p> <p><i>Not present</i></p>	<p>If present</p> <p>This field CAN contain dNSName. dNSName can be the same as the CN or any other FQDN. It can contain multiple FQDN's or wildcard OR this field CAN contain the Subject's mailbox.</p>	<p>Certificate Management Tool: Manual, but matched against a ruleset</p>
CRL Distribution Point	<p>c = no; CRL HTTP URL = http://crl.efos.se/SwedishPublicSectorFunctionCAv1.crl (2.5.29.31)</p>		CA
Programs principle	<p>c = no; [1] Program Certificate Policy: Principidentifierare = Client Authentication</p> <p>OR</p> <p>[1] Program Certificate Policy: Principidentifierare = Client Authentication [2] Program Certificate Policy: Principidentifierare = Server Authentication</p> <p>OR</p> <p>[1] Program Certificate Policy: Principidentifierare = Secure E-Mail</p> <p>OR <i>If Key</i> <i>Usage=nonRepudiation</i></p> <p>[1] Program Certificate Policy: Principidentifierare = Document Signing</p>	<p>This field MUST contain</p> <p>Client Authentication</p> <p>OR</p> <p>Client Authentication AND Server Authentication</p> <p>OR</p> <p>Secure E-Mail]</p> <p>OR <i>If Key</i> <i>Usage=nonRepudiation</i></p> <p>Document Signing</p>	<p>Certificate Management Tool based on CA templates</p>
Authority Information Access	<p>c = no; [1] Access to issuers information Access Method = Publisher of CA (1.3.6.1.5.5.7.48.2) Alternative Names: URL=http://aia.efos.se</p>		CA

	/SwedishPublicSectorFunctionCAv1.crt [2]Åtkomst till information om utfärdare Åtkomstmetod=Statusprotokoll för onlinercertifikat (1.3.6.1.5.5.7.48.1) Alternativt namn: URL= http://ocsp.efos.se		
--	--	--	--