

RPA End Entity Certificates

Version	Date	Change
1.3	2022-12-22	Authentication cert: Add OID 1.3.6.1.4.1.311.25.2 for SID (Security Identifier) from affiliated organizations active directory
1.2	2021-09-22	V1 to v2, add OU and removed serialnumber from Sign cert
1.1	2021-05-10	Change in SerialNumber from 18XXX to 19XXX

Authentication certificate

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 RPA CA v2 O = Swedish Social Insurance Agency C = SE		CA
Validity Period	Up to 36 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 RPA number will be given in the following format: 19XXXXXXXXXX	
Title	subject:title (2.5.4.12)	This field MUST contain the Subject's EFOS ID from EFOS Portal	Certificate Management Tool
Given Name	subject:givenName (2.5.4.42)	This field MUST contain "RPA"	
Sur Name	subject:surname (2.5.4.4)	This field MUST contain a number of the RPA	
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain the Subject's common name.	Certificate Management Tool: Combination of Given Name and Surname
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records.	Certificate Management Tool: Companies Registration Office and Central Bureau of Statistics
OrganizationUnit	subject:organizationUnitName (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: XXXXXXXXXXXX.	Certificate Management Tool: Companies Registration Office and Central Bureau of Statistics
Locality	subject:localityName (2.5.4.7)	This field MUST contain the locality/municipality of the headoffice for the	Certificate Management Tool: Companies Registration Office

		Subject's organization as listed in the official records	and Central Bureau of Statistics
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 and Central Bureau of Statistics
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)		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
1.2.752.34.2.1 Card Number Extension	19 digits	This field MUST contain 19 digits.	Certificate Management Tool
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)	Critical	CA
Extended Key Usage	c=no; Client Authentication (1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	This field MUST contain Client Authentication AND contain the smartCardLogon.	Certificate Management Tool based on CA templates
1.3.6.1.4.1.311.25.2	c=no; Octetstring (max 28)	IF present this field contain the Subject SID (Security Identifier) from affiliated organizations active directory.	Active directory
Certificate Policies	c=no; [1]Certificate Policy: Policy Identifier= OID 1.2.752.146.260.2 : https://repository.efos.se		
Subject Alternative Name	c=no; UPN = 19XXXXXXXXXX@organization.se OR RPA.XXXX@organization.se OR Not present	IF present this field CAN contain the RPAs number formatted as the subject's full Swedish social security number (or equal) OR mailbox and the agency domain name	Certificate Management Tool based on CA templates
CRL Distribution Point	c = no; CRL HTTP URL = https://crl.efos.se/ SwedishPublicSectorRPACAv2.crl (2.5.29.31)		CA
Programs principle	c=no; [1] Program Certificate Policy: Principidentifierare = Client Authentication [2] Program Certificate Policy:	This field MUST contain Client Authentication AND contain the smartCardLogon	Certificate Management Tool based on CA templates

	Principidentifierare = Smart Card Logon		
Authority Information Access	<p>c=no;</p> <p>[1]Åtkomst till information om utfärdare Åtkomstmetod=Utgivare av certifikatutfärdare (1.3.6.1.5.5.7.48.2) Alternativt namn: URL= https://aia.efos.se/SwedishPublicSectorRPACAv2.crt</p> <p>[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</p>		CA

Signing certificate

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 RPA CA v2 O = Swedish Social Insurance Agency C = SE		CA
Validity Period	Up to 36 months expressed in UTC format		Certificate Management Tool based on CA templates
Subject Distinguished Name			
Title	subject:title (2.5.4.12)	This field MUST contain the Subject's EFOS ID from EFOS Portal	Certificate Management Tool
Given Name	subject:givenName (2.5.4.42)	This field MUST contain "RPA"	
Sur Name	subject:surname (2.5.4.4)	This field MUST contain a number of the RPA	
Common Name	subject:commonName (2.5.4.3) cn = Common name	This field MUST contain the Subject's common name.	Certificate Management Tool: Combination of Given Name and Surname
Organization	subject:organizationName (2.5.4.10)	This field MUST contain the Subject's full legal organization name as listed in the official records.	Certificate Management Tool: Companies Registration Office and Central Bureau of Statistics
OrganizationUnit	subject:organizationUnitName (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: XXXXXXXXXX.	Certificate Management Tool: Companies Registration Office and 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 and Central Bureau of Statistics
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 and Central Bureau of Statistics
Subject Public Key Information	2048-bit RSA key modulus, rsaEncryption (1.2.840.113549.1.1.1)		CA
Issuer's Signature	sha256 WithRSAEncryption		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
1.2.752.34.2.1 Card Number Extension	19 digits	This field MUST contain 19 digits.	Certificate Management Tool
Key Usage	c=yes; nonRepudiation (40)	Critical	CA
Extended Key Usage	c=no; Document Signing (1.3.6.1.4.1.311.10.3.12)	This field MUST contain Document Signing	CA
Certificate Policies	c=no; [1]Certificate Policy: Policy Identifier= OID 1.2.752.146.260.2 : https://repository.efos.se		
CRL Distribution Point	c = no; CRL HTTP URL = https://crl.efos.se/SwedishPublicSectorRPACAv2.crl (2.5.29.31)		CA
Programs principle	c=no; [1] Program Certificate Policy: Principidentifierare = Document Signing	This field MUST contain Document Signing	CA
Authority Information Access	c=no; [1]Åtkomst till information om utfärdare Åtkomstmetod=Utgivare av certifikatutfärdare (1.3.6.1.5.5.7.48.2) Alternativt namn: URL= https://aia.efos.se/SwedishPublicSectorRPACAv2.crt [2]Åtkomst till information om utfärdare Åtkomstmetod=Statusprotokoll för onlinecertifikat (1.3.6.1.5.5.7.48.1) Alternativt namn: URL=http://ocsp.efos.se		CA