

EFOS End Entity Mobile ID Certificates

Version	Date	Change
1.5	2021-02-22	Authentication cert: Removing Email. Change in SAN
1.4	2020-12-21	Authentication cert: Adding Title (Subject) Signing cert: Removing SerialNumber + Adding Title (Subject)

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 Mobile ID 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 full Swedish social security number (or equal) Social Security Number will be given in the following format: YYYYMMDDXXXX	Certificate Management Tool: 1: Tax Agency 2: Internal database for Sequence Numbers
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 the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent	Certificate Management Tool: 1: Tax Agency
Sur Name	subject: surname (2.5.4.4)	This field MUST contain all of the Subject's surnames.	Certificate Management Tool: 1: Tax Agency
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	Certificate Management Tool:

		name as listed in the official records.	Companies Registration Office and Central Bureau of Statistics
OrganizationUnit	subject:organizationUnit Name (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 (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	14 digits	This field MUST contain 14 digits.	Certificate Management Tool based on device. Not a card number from Card Supplier
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)	This field MUST contain Client Authentication	Certificate Management Tool based on CA templates
Subject Alternative Name	c=no; UPN = YYYYMMDDNNNN@organization.se OR Not present	IF present this field CAN contain the Subject's User Principal Name formatted as the subject's full Swedish social security number (or equal) OR mailbox and the agency domain name OR Not present	Certificate Management Tool based on CA templates
Certificate Policies	c=no;	OID: Mobile ID CA v1 = 1.2.752.146.250.3	Certificate Management Tool based on CA templates

	[1]Certificate Policy: Policy Identifier= 1.2.752.146.250.3 https:// repository.efos.se		
CRL Distribution Point	c = no; CRL HTTP URL = http://crl.efos.se /SwedishPublicSectorMo bileIDCAv1.crl (2.5.29.31)		CA
Programs principle	c=no; [1] Program Certificate Policy: Principidentifierare = Client Authentication	This field MUST contain Client Authentication	Certificate Management Tool based on CA templates
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= http://aia.efos.se /SwedishPublicSectorMo bileIDCAv1.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

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 Mobile ID 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			
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 the Subject's marked Given Name IF it exists OR All Given Names of the subject if marking of Given Name is absent and First Names exists This field is empty if Given Name and First Names are absent	Certificate Management Tool: 1: Tax Agency
Sur Name	subject: surname (2.5.4.4)	This field MUST contain all of the Subject's surnames.	Certificate Management Tool: 1: Tax Agency
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 (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
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	Certificate Management Tool based on CA templates
Certificate Policies	c=no; [1]Certificate Policy: Policy Identifier= 1.2.752.146.250.3 https:// repository.efos.se	OID: Mobile ID CA v1 = 1.2.752.146.250.3	Certificate Management Tool based on CA templates
CRL Distribution Point	c = no; CRL HTTP URL = http://crl.efos.se/SwedishPublicSectorMobileIDCAv1.crl (2.5.29.31)		CA
Programs principle	c=no; [1] Program Certificate Policy: Principidentifierare = Document Signing	This field MUST contain Document Signing	Certificate Management Tool based on CA templates
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=http:// http://aia.efos.se/SwedishPublicSectorMobileIDCAv1.crt [2]Åtkomst till information om utfärdare Åtkomstmetod=Statusprotokoll för onlinecertifikat (1.3.6.1.5.5.7.48.1)		CA

	Alternativt namn: URL= http://ocsp.efos.se		
--	---	--	--