EFOS End Entity HSA Person 2-4 Certificates

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 = SEE RIGHT ->O = Swedish Social Insurance AgencyC = SE	CN = Swedish Public Sector HSA Person 2 CA v1 Swedish Public Sector HSA Person 3 CA v1 Swedish Public Sector HSA Person 4 CA v1	CA
Validity Period	Up to 60 months expressed in UTC format		Certificate Management Tool based on CA templates
Subject Distinguished Name			
Email	Subject:emailAddress (1.2.840.113549.1.9.1)	This field **CAN** contain the email address of the Subject	**Certificate Management Tool:** Fetched from HSA Directory
SerialNumber	Subject:serialNumber (2.5.4.5)	This field **MUST** contain the Subject's HSA-id in the following format: Alphanumerical and up to 31 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:** Fetched from HSA Directory
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 **2:** Inera Personal Identity Service

Sur Name	subject: surname (2.5.4.4)	This field **MUST** contain all of the Subject's surnames.	**Certificate Management Tool:** **1:** Tax Agency **2:** Inera Personal Identity Service
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
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 (1.2.840.113549.1.1.1)		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.	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) **AND/OR** Smart Card Logon (1.3.6.1.4.1.311.20.2.2) **AND/OR** Secure E-Mail (1.3.6.1.5.5.7.3.4)	This field **MUST** contain Client Authentication It **CAN** also contain smartCardLogon **AND/OR** emailProtection if subject has a mailbox and/or UPN at the organization.	Certificate Management Tool based on CA templates
Certificate Policies	c=no; [1]Certificate Policy: Policy	HSA Person 2 CA v1 – OID 1.2.752.146.260.2.Z HSA Person 3 CA v1 – OID 1.2.752.146.270.3.Z	Certificate Management Tool based on CA templates

	Identifier=2.23.140.1.2.3 [2]Certificate Policy: Policy Identifier= SEE RIGHT-> [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.efos.se	HSA Person 4 CA v1 – OID 1.2.752.146.280.4.Z Where Z points to the specific issuance routine that was used	
Subject Alternative Name	c=no; UPN = username@domain.suffix **AND/OR** RFC822Name = mailbox@domain.suffix **OR** Not present	**IF** present this field **CAN** contain The subject's User Principal Name **AND/OR** The subject's Email Address as RFC822Name	**Certificate Management Tool:** Fetched from HSA Directory
CRL Distribution Point	c = no; CRL HTTP URL = SEE RIGHT -> (2.5.29.31)	http://crl.efos.se/SwedishPublicSectorHSAPerson2CAv1.crl **OR** http://crl.efos.se/SwedishPublicSectorHSAPerson3CAv1.crl **OR** http://crl.efos.se/SwedishPublicSectorHSAPerson4CAv1.crl	CA
Programs principle	c=no; [1] Program Certificate Policy: Principidentifierare = Client Authentication **AND/OR** [2] Program Certificate Policy: Principidentifierare = Smart Card Logon **AND/OR** [3] Program Certificate Policy: Principidentifierare = Secure E-Mail	This field **MUST** contain Client Authentication **AND CAN** contain the smartCardLogon and/or emailProtection if subject has a mailbox and/or UPN at the organization.	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= SEE RIGHT->[2]Åtkomst till information om utfärdare	http://aia.efos.se/SwedishPublicSectorHSAPerson2CAv1.crt **OR** http://aia.efos.se/SwedishPublicSectorHSAPerson3CAv1.crt **OR** http://aia.efos.se/SwedishPublicSectorHSAPerson4CAv1.crt	CA

	Åtkomstmetod=Statusprotokoll för onlinecertifikat (1.3.6.1.5.5.7.48.1) Alternativt namn: URL=http://ocsp.efos.se		

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 = SEE RIGHT->O = Swedish Social Insurance Agency C = SE	CN = Swedish Public Sector HSA Person 2 CA v1 Swedish Public Sector HSA Person 3 CA v1 Swedish Public Sector HSA Person 4 CA v1	CA
Validity Period	Up to 60 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 HSA-id in the following format: Alphanumerical and up to 31 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:** HSA Directory
Given Name	subject:givenName (2.5.4.42)	This field **MUST** contain the Subject's name 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 Names and First Names are absent	**Certificate Management Tool:** **1:** Tax Agency **2:** Inera Personal Identity Service
Sur Name	subject: surname (2.5.4.4)	This field **MUST** contain all of the Subject's surnames.	**Certificate Management Tool:** **1:** Tax Agency **2:** Inera Personal Identity Service
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
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	19 digits	This field **MUST** contain 19 digits.	Card Supplier
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=2.23.140.1.2.3 [2]Certificate Policy: Policy Identifier=SEE RIGHT ->[2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.efos.se	HSA Person 2 CA v1 – OID 1.2.752.146.260.2.Z HSA Person 3 CA v1 – OID 1.2.752.146.270.3.Z HSA Person 4 CA v1 – OID 1.2.752.146.280.4.Z Where Z points to the specific issuance routine that was used	Certificate Management Tool based on CA templates
CRL Distribution Point	c = no; CRL HTTP URL = SEE RIGHT ->(2.5.29.31)	http://crl.efos.se/SwedishPublicSectorHSAPerson2CAv1.crl **OR** http://crl.efos.se/SwedishPublicSectorHSAPerson3CAv1.crl **OR**	CA

		http://crl.efos.se /SwedishPublicSectorHSA Person4CAv1.crl	
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:// SEE RIGHT -> [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	http://aia.efos.se /SwedishPublicSectorHSA Person2CAv1.crt **OR** http://aia.efos.se /SwedishPublicSectorHSA Person3CAv1.crt **OR** http://aia.efos.se /SwedishPublicSectorHSA Person4CAv1.crt	CA