POINTSHARP

Certificate specifications

Pointsharp Net iD svensk e-legitimation

Digitally
signed by PsPT
Date:
2024.05.24
15:25:52
+02'00'

Classification:	Internal
Publication No.:	PSC-Rd22-02
Document version:	1.4
Document status:	Final
Date:	13 May 2024

Table of Contents

1 Net iD SweID · Introduction

This section intentionally left blank.

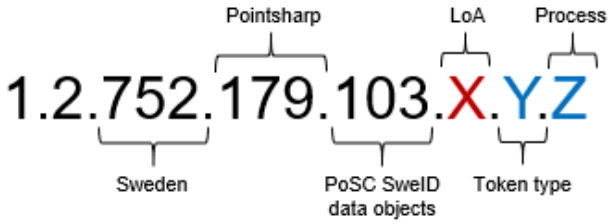
2 Net iD SweID · Attribute descriptions

This section intentionally left blank.

3 Net iD SweID · Content relationship between certificate and HSA

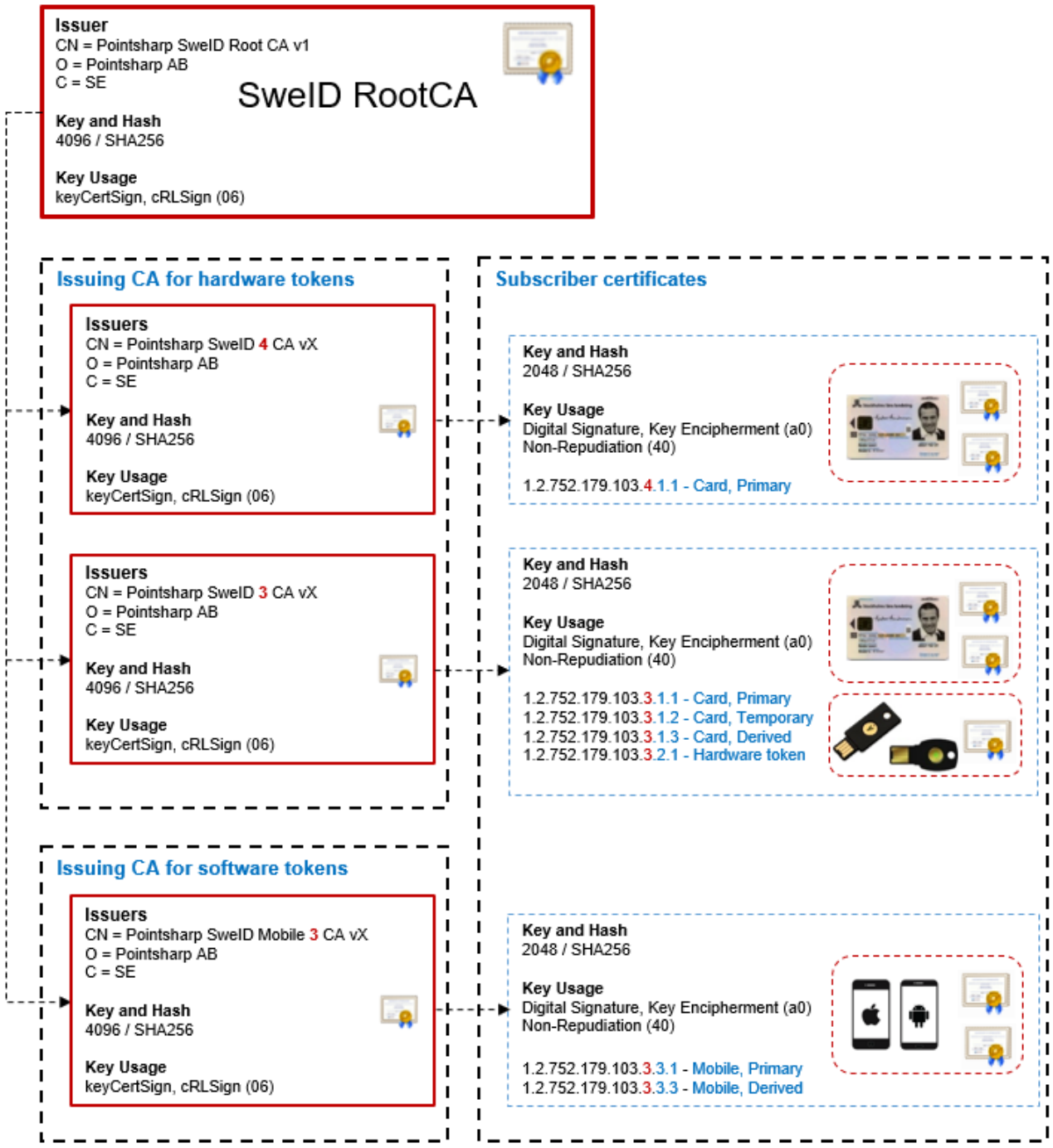
This section intentionally left blank.

4 Net iD SweID – Certificate specifications



LoA	Token type	Process
3 4	1 = Smart card 2 = Hardware token 3 = Mobile (app)	1 = Primary 2 = Temporary 3 = Derived credentials

1 SweID CA OIDs



2 SweID CA hierarchy

4.1 SweID Root CA certificate

1 Pointsharp SweID Root CA v1

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment	
Version	3	n/a	Integer		
serialNumber	Randomized	n/a	Integer		
signatureAlgorithm	sha-256WithRSAEncryption (1.2.840.113549.1.1.11)	n/a	n/a (null)		
Issuer		n/a	n/a		
commonName (2.5.4.3)	Pointsharp SweID Root CA v1		UTF8String		
organizationName (2.5.4.10)	Pointsharp AB		UTF8String		
countryName (2.5.4.6)	SE		PrintableString		
Validity	25 years	n/a	n/a		
notBefore	<Root CA certificate issuing date>		UTCTime		
notAfter	<notBefore + 25 years>		UTCTime		
Subject		n/a			

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment	
commonName (2.5.4.3)	Pointsharp SweID Root CA v1		UTF8String		
organizationName (2.5.4.10)	Pointsharp AB		UTF8String		
countryName (2.5.4.6)	SE		PrintableString		
subjectPublicKeyInfo		n/a	n/a		
algorithm	rsaEncryption {1.2.840.113549.1.1.1}		n/a (null)		
subjectPublicKey	Public key, RSA 4096 bits		BIT STRING		
subjectKeyIdentifier (2.5.29.14)		NC	n/a		
keyIdentifier	Hash of part of the Root CA's public key		OCTET STRING		
keyUsage (2.5.29.15)	keyCertSign, cRLSign (06)	C	OCTET STRING		
basicConstraints (2.5.29.19)	Subject Type=CA Path Length Constraint=1	C	OCTET STRING, Bolean, integer		

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment	
Signature	RSA signature with SHA-256	n/a	BIT STRING		

4.2 SweID Issuing CAs

2 Pointsharp SweID CAs

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment
Version	3	n/a	Integer	
serialNumber	Randomized	n/a	Integer	
signatureAlgorithm	sha-256WithRSAEncryption (1.2.840.113549.1.1.11)	n/a	n/a (null)	
Issuer		n/a	n/a	
commonName (2.5.4.3)	Pointsharp SweID Root CA v1		UTF8String	
organizationName (2.5.4.10)	Pointsharp AB		UTF8String	
countryName (2.5.4.6)	SE		PrintableString	
Validity	12 years	n/a	n/a	
notBefore	<CA certificate issuing date>		UTCTime	
notAfter	<notBefore + 12 years>		UTCTime	
Subject		n/a		

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment
commonName (2.5.4.3)	Depending on the Issuing CA. Must be one of the following: • Pointsharp SweID 4 CA vX • Pointsharp SweID 3 CA vX • Pointsharp SweID Mobile 3 CA vX		UTF8String	'X' in the CA names represents a digit for the CA version.
organizationName (2.5.4.10)	Pointsharp AB		UTF8String	
countryName (2.5.4.6)	SE		PrintableString	
subjectPublicKeyInfo		n/a	n/a	
algorithm	rsaEncryption {1.2.840.113549.1.1.1}		n/a (null)	
subjectPublicKey	Public key, RSA 4096 bits		BIT STRING	
cRLDistributionPoints (2.5.29.31)	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http:// crl.pointsharpsecurecloud.com/ pointsharpsweidrootcav1.crl	NC	OCTET STRING	

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment
authorityInformationAccess (1.3.6.1.5.5.7.1.1)	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.pointsharpsecurecloud.com [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.pointsharpsecurecloud.com/pointsharpsweidrootcav1.cer	NC	OCTET STRING	
certificatePolicies (2.5.29.32)	[1]Certificate Policy: Policy Identifier=1.2.752.179.100.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.pointsharpsecurecloud.com	NC	OCTET STRING CPS Qualifier=IA5 string	
subjectKeyIdentifier (2.5.29.14)		NC	n/a	
keyIdentifier	Hash of part of the Issuing CA's public key		OCTET STRING	
authorityKeyIdentifier		NC	n/a	

Attribute (OID)	Value	Critical/Non-critical	Data type	Comment
keyIdentifier	Contains the subjectKeyIdentifier of 'Pointsharp SweID Root CA v1'. Hash of part of the Root CA's public key.		OCTET STRING	
keyUsage (2.5.29.15)	keyCertSign, cRLSign (06)	C	OCTET STRING	
basicConstraints (2.5.29.19)	Subject Type=CA Path Length Constraint=0	C	OCTET STRING, Bolean, integer	
Signature	RSA signature with SHA-256	n/a	BIT STRING	

4.3 SweID Subscriber certificates - Individuals

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
Version	1	3		CA	M	n/a	Integer	
serialNumber	64	Randomized	7899f9a6128e298 24c8bccf757f06f16	CA	M	n/a	Integer	
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		CA	M	n/a	n/a (null)	
Issuer						n/a		
commonName (2.5.4.3)		Depending on the Issuing CA. Must be one of the following: • Pointsharp SweID 4 CA vX • Pointsharp SweID 3 CA vX • Pointsharp SweID Mobile 3 CA vX		CA	M		UTF8String	'X' in the CA names represents a digit for the CA version.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
organizationName (2.5.4.10)		Pointsharp AB		CA	M		UTF8String	
countryName (2.5.4.6)		SE		CA	M		PrintableString	
Validity		minimum 1 day, maximum 5 years				n/a	n/a	
notBefore	13	<Subscriber certificate issuing date>	200301011030Z	CA	M		UTCTime	
notAfter	13	<notBefore + Validity>	250301011030Z	CA	M		UTCTime	
Subject						n/a		

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
serialNumber (2.5.4.5)	64		195704133106	RA/CA SPAR	M*		PrintableString	Given by RA/CA officer and verified with SPAR. SPAR = Swedish Tax Agency's register with individuals living in Sweden and having a Swedish personal id number ("personnummer" or "samordningsnummer". * Mandatory in authentication certificates (keyUsage='A0').
givenName (2.5.4.42)	64		Lena Sofia	SPAR	M**		UTF8String	Given names according to SPAR. ** Not included for individuals that have no given name.
surName (2.5.4.4)	64		Svensson	SPAR	M		UTF8String	Middle name & surname according to SPAR.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
commonName (2.5.4.3)	64		Lena Svensson	SPAR	M		UTF8String	First name and surname according to SPAR. If no flag exists for first name in SPAR the RA can choose from the given names registered in SPAR.
title (2.5.4.12)	64	<Subscriber PoSC ID>	4711	CA	M		UTF8String	Subscriber PoSC ID is an additional numeric ID automatically assigned to the subscriber by the PoSC Portal (system). The PoSC ID is unique within the PoSC Portal and the CA. Is used to anonymize the "public" ID of the subscriber in a signature and still have a relation to the authentication certificate.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
organizationName (2.5.4.10)	64		Organization X	CA BV and SCB	M		UTF8String	Organization name and organization number verified with Companies Registration Office (Bolagsverket) and/or Central Bureau of Statistics (SCB: Statistiska Centralbyrån).
organizationalUnitName (2.5.4.11)	128		SE556671547901	CA	M		UTF8String	VAT number of the RA organization according to EU standard (VAT identification number). Also see notes above for organizationName.
organizationalUnitName (2.5.4.11)	128		HR	RA	O		UTF8String	An organizational unit within the RA organization related to the subscriber.
localityName (2.5.4.7)	128		Stockholm	CA	M		UTF8String	The main locality of the RA organization.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
countryName (2.5.4.6)	2		SE	CA	M		PrintableString	
Cardnumber extension (1.2.752.34.2.1)	19	<CardNumber according to Swedish standard SS614331>		Card Supplier or CA	M	NC	PrintableString	Hard and soft tokens not beeing "cards" will also be given a unique number in this extension.
subjectPublicKeyInfo						n/a	n/a	
Algorithm		rsaEncryption {1.2.840.113549.1.1.1}		CA	M		n/a (null)	
subjectPublicKey		Public key, RSA 2048 bits		CA	M		BIT STRING	

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
cRLDistribution Points (2.5.29.31)		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.pointsharpsecurecloud.com/<CN of Issuing CA in lowercase characters and without spaces>.crl	Full Name options depending on Issuing CA. Must be one of the following: URL=http://crl.pointsharpsecurecloud.com/pointsharpsweid4cavX.crl OR URL=http://crl.pointsharpsecurecloud.com/pointsharpsweid3cavX.crl OR URL=http://crl.pointsharpsecurecloud.com/pointsharpsweidmobile3cavX.crl	CA	M	NC	OCTET STRING	'X' in the CA names of the URLs represents a digit for the CA version.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
authorityInformationAccess (1.3.6.1.5.5.7.1.1)		[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repository.pointsharpsecurecloud.com/<CN of Issuing CA in lowercase characters and without spaces>.cer [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.pointsharpsecurecloud.com	Alternative Name options depending on Issuing CA. Must be one of the following: URL=http://repository.pointsharpsecurecloud.com/pointsharpsweid4cavX.cer OR URL=http://repository.pointsharpsecurecloud.com/pointsharpsweid3cavX.cer OR URL=http://repository.pointsharpsecurecloud.com/pointsharpsweidmobile3cavX.cer	CA	M	NC	OCTET STRING	'X' in the CA names of the URLs represents a digit for the CA version.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
subjectAltName (2.5.29.17)						NC		
userPrincipalName (1.3.6.1.4.1.311.20.2.3)	255		lensve@organizationx.se OR lena.svensson@organizationx.se	RA	O			For AD logon.
rfc822Name	255		lena.svensson@organizationx.se	RA	O			For secure e-mail.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
certificatePolicies (2.5.29.32)		[1]Certificate Policy: Policy Identifier=<OID according to examples> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.pointsharpsecurecloud.com	The OID of the Policy Identifier must be one of the following: • 1.2.752.179.10 3.4.1.1 - LoA4: Card, Primary • 1.2.752.179.10 3.3.1.1 - LoA3: Card, Primary • 1.2.752.179.10 3.3.1.2 - LoA3: Card, Temporary • 1.2.752.179.10 3.3.1.3 - LoA3: Card, Derived • 1.2.752.179.10 3.3.2.1 - LoA3: Hardware token • 1.2.752.179.10 3.3.3.1 - LoA3: Mobile, Primary • 1.2.752.179.10 3.3.3.3 - LoA3: Mobile, Derived	CA	M		OCTET STRING CPS Qualifier=IA 5 string	OID depending on the LoA issuing process and the key protection.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
enhancedKeyUsage (2.5.29.37)					M	NC		
clientAuthentication (1.3.6.1.5.5.7.3.2)				CA	M*			* Mandatory in authentication certificates (keyUsage='A0').
smartCardLogon (1.3.6.1.4.1.311.20.2.2)				CA	O***			*** Mandatory in authentication certificates (keyUsage='A0') if userPrincipleName is present.
emailProtection (1.3.6.1.5.5.7.3.4)				CA	O****			**** Mandatory in authentication certificates (keyUsage='A0') if rfc822Name is present.

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
documentSigning (1.3.6.1.4.1.311.10.3.12)				CA	M*****			***** Mandatory in signature certificates (keyUsage='40').
Microsoft SID extension (1.3.6.1.4.1.311.25.2)		SID from RA's local AD	S-1-5-21-3002805517-771439646-35828631	RA	M*	NC	OCTET STRING	* Mandatory in authentication certificates (keyUsage='A0').
subjectKeyIdentifier (2.5.29.14)						NC	n/a	
keyIdentifier		Hash of part of the subscriber's certificates public key					OCTET STRING	
authorityKeyIdentifier (2.5.29.35)						NC	n/a	

Attribute (OID)	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
keyIdentifier		subjectKeyIdentifier of the Issuing CA. Hash of part of the Issuing CA's public key.		CA			OCTET STRING	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment (A0) OR Non-Repudiation (40)		CA	M	C	OCTET STRING	
Signature		RSA signature with SHA-256		CA	M	n/a	BIT STRING	

4.4 SweID CRL Profile

4.4.1 Version number(s)

PoSC Net iD issues X.509 version 2 CRLs that conform to RFC5280.

4.4.2 CRL and CRL entry extensions

PoSC Net iD CRL extensions conform to the Extensions profile in RFC5280.

3 Certificate revocation lists (CRLs)

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
Version	2	V2		n/a	Integer	
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		n/a	n/a (null)	
Issuer				n/a		
commonName (2.5.4.3)		Depending on the Issuing CA. Must be one of the following: • Pointsharp SweID 4 CA vX • Pointsharp SweID 3 CA vX • Pointsharp SweID Mobile 3 CA vX			UTF8String	'X' in the CA names represents a digit for the CA version.
organizationName (2.5.4.10)		Pointsharp AB			UTF8String	
countryName (2.5.4.6)		SE			PrintableString	
This Update	13	<CRL issuing date and time>	201012113230Z	n/a	UTCTime	
Next Update	13	<This Update + 24 hours>	201014113230Z	n/a	UTCTime	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
CRL Number	Up to 20 octets			NC	Integer	
authorityKeyIdentifier				NC		
keyIdentifier		Contains the subjectKeyIdentifier of the Isuing CA. Hash of part of the Issuing CA's public key.			OCTET STRING	
Signature		RSA signature with SHA-256		n/a	BIT STRING	

4.5 SweID OCSP Responder certificates

4.5.1 Version number(s)

PoSC Net iD uses the OCSP specification as defined by RFC6960.

4.5.2 OCSP extensions

PoSC Net iD only uses OCSP extensions that conform to the Extensions profile in RFC6960.

4 Certificates for OCSP signing

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
Version	1	3		n/a	Integer	
serialNumber	64	Randomized	015210445c0117512d07ce449da81d	n/a	Integer	
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		n/a	n/a (null)	
Issuer				n/a		
commonName (2.5.4.3)		Depending on the Issuing CA. Must be one of the following: • Pointsharp SweID 4 CA vX • Pointsharp SweID 3 CA vX • Pointsharp SweID Mobile 3 CA vX			UTF8String	'X' in the CA names represents a digit for the CA version.
organizationName (2.5.4.10)		Pointsharp AB			UTF8String	
countryName (2.5.4.6)		SE			PrintableString	
Validity		3 months		n/a	n/a	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
notBefore	13	<ocsp certificate issuing date>	200801011030Z		UTCTime	
notAfter	13	<notBefore + 3 months>	201101011030Z		UTCTime	
Subject				n/a		
commonName (2.5.4.3)	64	<CN of Issuing CA> OCSP Responder Z	Pointsharp SweID 4 CA vX OCSP Responder 1		UTF8String	'X' in the CA names represents a digit for the CA version and 'Z' represents a digit for the instance number of the responder.
organizationName (2.5.4.10)	64	Pointsharp AB			UTF8String	
countryName (2.5.4.6)	2	SE			PrintableString	
subjectPublicKeyInfo				n/a	n/a	
Algorithm		rsaEncryption {1.2.840.113549.1.1.1}			n/a (null)	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
subjectPublicKey		Public key, RSA 2048			BIT STRING	
OCSP No Revocation Checking		05 00		NC	OCTET STRING	
enhancedKeyUsage				NC		
OCSPSigning (1.3.6.1.5.5.7.3.9)						
subjectKeyIdentifier (2.5.29.14)				NC	n/a	
keyIdentifier		Hash of part of the OCSP Responder's public key			OCTET STRING	
authorityKeyIdentifier				NC	n/a	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
keyIdentifier		Contains the subjectKeyIdentifier of the Isuing CA. Hash of part of the Issuing CA's public key.			OCTET STRING	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment (A0)		C	OCTET STRING	
Signature		RSA signature with SHA-256		n/a	BIT STRING	

4.6 SweID Root CA ARL Profile

4.6.1 Version number(s)

PoSC Net iD issues X.509 version 2 CRLs that conform to RFC5280.

4.6.2 CRL and CRL entry extensions

PoSC Net iD CRL extensions conform to the Extensions profile in RFC5280.

5 Certificate revocation lists (CRLs)

Attribute (OID)	Max length	Value	Example	Critical/Non-critical	Data type
Version	2	V2		n/a	Integer
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		n/a	n/a (null)
Issuer				n/a	
commonName (2.5.4.3)		Pointsharp SweID Root CA v1			UTF8String
organizationName (2.5.4.10)		Pointsharp AB			UTF8String
countryName (2.5.4.6)		SE			PrintableString
This Update	13	<CRL issuing date and time>	201012113230Z	n/a	UTCTime
Next Update	13	<This Update + 1 year>	211012113230Z	n/a	UTCTime
CRL Number	Up to 20 octets			NC	Integer
authorityKeyIdentifier				NC	

Attribute (OID)	Max length	Value	Example	Critical/Non-critical	Data type
keyIdentifier		Contains the subjectKeyIdentifier of 'Pointsharp SweID Root CA v1'. Hash of part of the Root CA's public key.			OCTET STRING
Signature		RSA signature with SHA-256		n/a	BIT STRING

4.7 SweID Root CA OCSP Responder certificates

4.7.1 Version number(s)

PoSC Net iD uses the OCSP specification as defined by RFC6960.

4.7.2 OCSP extensions

PoSC Net iD only uses OCSP extensions that conform to the Extensions profile in RFC6960.

6 Certificates for OCSP signing

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
Version	1	3		n/a	Integer	
serialNumber	64	Randomized	015210445c0117512d07ce449da81d	n/a	Integer	
signatureAlgorithm		sha-256WithRSAEncryption (1.2.840.113549.1.1.11)		n/a	n/a (null)	
Issuer				n/a		
commonName (2.5.4.3)		Pointsharp SweID Root CA v1			UTF8String	
organizationName (2.5.4.10)		Pointsharp AB			UTF8String	
countryName (2.5.4.6)		SE			PrintableString	
Validity		1 year		n/a	n/a	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
notBefore	13	<ocsp certificate issuing date>	211012113230Z		UTCTime	
notAfter	13	<notBefore + 1 year>	221012113230Z		UTCTime	
Subject				n/a		
commonName (2.5.4.3)	64	Pointsharp SweID Root CA v1 OCSP Responder Z	Pointsharp SweID Root CA v1 OCSP Responder 1		UTF8String	'Z' represents a digit for the instance number of the responder.
organizationName (2.5.4.10)	64	Pointsharp AB			UTF8String	
countryName (2.5.4.6)	2	SE			PrintableString	
subjectPublicKeyInfo				n/a	n/a	
Algorithm		rsaEncryption {1.2.840.113549.1.1.1}			n/a (null)	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
subjectPublicKey		Public key, RSA 2048			BIT STRING	
OCSP No Revocation Checking		05 00		NC	OCTET STRING	
enhancedKeyUsage				NC		
OCSPSigning (1.3.6.1.5.5.7.3.9)						
subjectKeyIdentifier (2.5.29.14)				NC	n/a	
keyIdentifier		Hash of part of the OCSP Responder's public key			OCTET STRING	
authorityKeyIdentifier				NC	n/a	

Attribute (OID)	Max length	Value	Example	Critical/ Non-critical	Data type	Comments
keyIdentifier		Contains the subjectKeyIdentifier of 'Pointsharp SweID Root CA v1'. Hash of part of the Root CA's public key.			OCTET STRING	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment (A0)		C	OCTET STRING	
Signature		RSA signature with SHA-256		n/a	BIT STRING	

Website
https://www.pointsharp.com

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification:	Internal
Publ. No.:	PSC-Rd22-02
Document version:	1.4
Document status:	Final
OID:	
Published:	13 May 2024