POINTSHARP

Certificate specifications

Pointsharp Net iD

Digitally signed by PsPT
Date: 2024.05.24
15:26:56 +02'00'

Classification:	Public
Publication No.:	PSC-Rd21-02
Document version:	2.1
Document status:	Final
Date:	24 Mar 2023

Table of Contents

1 Introduction

This section intentionally left blank.

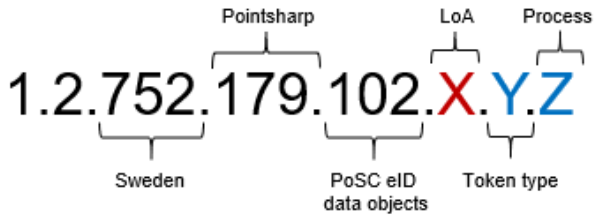
2 Attribute descriptions

This section intentionally left blank.

3 Content relationship between certificate and HSA

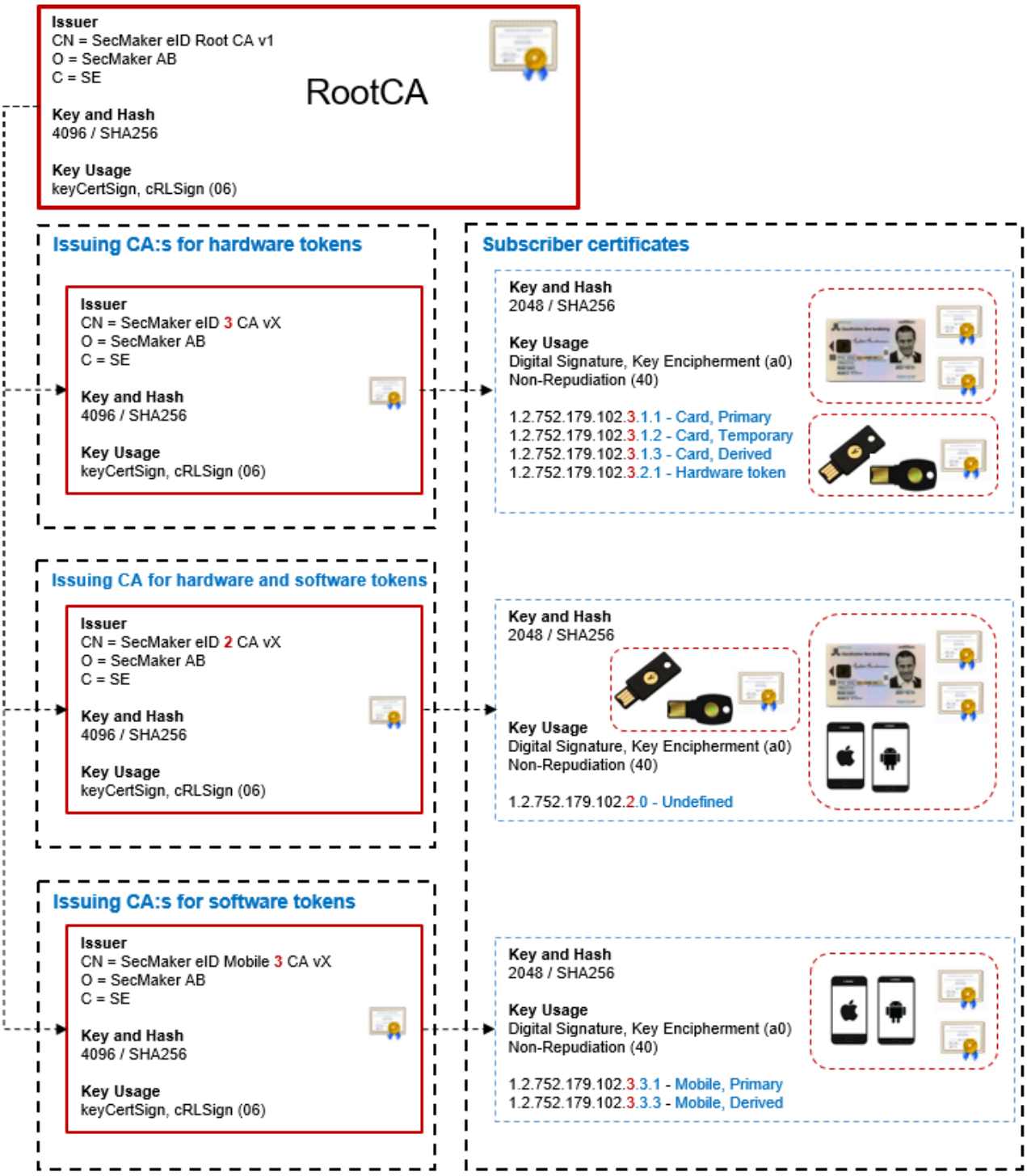
This section intentionally left blank.

4 eID - certificate specifications



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

1 eID CA OIDs



2 eID CA hierarchy

4.1 eID Root CA certificate

1 SecMaker eID 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)	SecMaker eID Root CA v1		UTF8String		
organizationName (2.5.4.10)	SecMaker 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)	SecMaker eID Root CA v1		UTF8String		
organizationName (2.5.4.10)	SecMaker 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 eID Issuing CAs

2 Pointsharp eID 3 CA vX / Pointsharp eID Mobile 3 CA vX / Pointsharp eID 2 CA vX

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)	SecMaker eID Root CA v1		UTF8String	
organizationName (2.5.4.10)	SecMaker AB		UTF8String	
countryName (2.5.4.6)	SE		PrintableString	
Validity	12 years	n/a	n/a	
notBefore	<CA certificate issuing date>		UTCTime	

Attribute (OID)	Value	Critical /Non-critical	Data type	Comment
notAfter	<notBefore + 12 years>		UTCTime	
Subject		n/a		
commonName (2.5.4.3)	Depending on the Issuing CA. Must be one of the following: • Pointsharp eID 3 CA vX • Pointsharp eID Mobile 3 CA vX • Pointsharp eID 2 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)	

Attribute (OID)	Value	Critical /Non-critical	Data type	Comment
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/secmakereidrootcav1.crl	NC	OCTET STRING	
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/secmakereidrootcav1.cer	NC	OCTET STRING	

Attribute (OID)	Value	Critical /Non-critical	Data type	Comment
certificatePolicies (2.5.29.32)	[1]Certificate Policy: Policy Identifier=1.2.752.179.100.2.2 [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	
keyIdentifier	Contains the subjectKeyIdentifier of 'SecMaker eID 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	

Attribute (OID)	Value	Critical /Non-critical	Data type	Comment
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 eID Subscriber certificates - Individuals

* Not included for individuals that have no given name.

	Maxlength	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
Version	1	3		CA	M	n/a	Integer	
serialNumber	64	Randomized	7899f9a6128e29824c8bccf757f06f16	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 eID 3 CA vX • Pointsharp eID Mobile 3 CA vX • Pointsharp eID 2 CA vX		CA	M		UTF8String	'X' in the CA names represents a digit for the CA version.
organizationName (2.5.4.10)		Pointsharp AB		CA	M		UTF8String	

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
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 and time>	230301011030Z	CA	M		UTCTime	
notAfter	13	<notBefore + Validity>	280301011030Z	CA	M		UTCTime	
Subject						n/a		
serialNumber (2.5.4.5)	64		PS07536	RA	M/O**		PrintableString	** Mandatory to have Subject serialNumber OR userPrincipalName present in the certificate.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
givenName (2.5.4.42)	64		Lena Sofia	RA	M*		UTF8String	The given names of the subscriber. * Not included for individuals that have no given name.
surName (2.5.4.4)	64		Svensson	RA	M		UTF8String	The middle names and surnamn of the subscriber.
commonName (2.5.4.3)	64		Lena Svensson	RA	M		UTF8String	A 'friendly name' of the subscriber. The first name and surname of the subscriber.
title (2.5.4.12)	64	<Subscriber PoSC ID>	4711	CA	O		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 normally included in the certificate but may be omitted.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
organizationName (2.5.4.10)	64		Organization X	CA	M		UTF8String	Official name of the RA organization.
organizationalUnitName (2.5.4.11)	128		SE556691063301 OR SEBOLREG.5566910633	CA	M		UTF8String	The VAT identification number of the RA organization if such exists, alternatively the EUID.
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.
countryName (2.5.4.6)	2		SE	CA	M		PrintableString	The country where the RA organization has its main business.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
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	

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
cRLDistributionPoints (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/pointsharpeid3cavX.crl OR URL=http://crl.pointsharpsecurecloud.com/pointsharpeidmobile3cavX.crl OR URL=http://crl.pointsharpsecurecloud.com/pointsharpeid2cavX.crl	CA	M	NC	OCTET STRING	'X' in the CA names of the URLs represents a digit for the CA version.

	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/pointsharpeid3cavX.cer OR URL=http://repository.pointsharpsecurecloud.com/pointsharpeidmobile3cavX.cer OR URL=http://repository.pointsharpsecurecloud.com/pointsharpeid2cavX.cer	CA	M	NC	OCTET STRING	'X' in the CA names of the URLs represents a digit for the CA version.
subjectAltName (2.5.29.17)						NC		

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
userPrincipalName (1.3.6.1.4.1.311.20.2.3)	255		lensve@pointsharp.com OR lena.svensson@pointsharp.com	RA	M/O**			For AD logon. ** Mandatory to have Subject serialNumber or userPrincipalName present in the certificate.
rfc822Name	255		lena.svensson@pointsharp.com	RA	O			For secure e-mail.

	Maxlength	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: • 1.2.752.179.102.3.1.1 - LoA3: Card, Primary • 1.2.752.179.102.3.1.2 - LoA3: Card, Temporary • 1.2.752.179.102.3.1.3 - LoA3: Card, Derived • 1.2.752.179.102.3.2.1 - LoA3: Hardware token • 1.2.752.179.102.3.3.1 - LoA3: Mobile, Primary • 1.2.752.179.102.3.3.3 - LoA3: Mobile, Derived • 1.2.752.179.102.2.0.5 - LoA2: Undefined, User	CA	M		OCTET STRING CPS Qualifier=IA5 string	OID depending on the LoA issuing process and the key protection.
enhancedKeyUsage					M	NC		

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
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 authentication certificates (keyUsage='A0') if rfc822Name is present.
documentSigning (1.3.6.1.4.1.311.10.3.12)				CA	M*****			***** Mandatory in signature certificates (keyUsage='40').

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
subjectKeyIdentifier (2.5.29.14)						NC	n/a	
keyIdentifier		Hash of part of the subscriber's public key			M		OCTET STRING	
authorityKeyIdentifier						NC	n/a	
keyIdentifier		subjectKeyIdentifier of the Issuing CA. Hash of part of the Issuing CA's public key.		CA	M		OCTET STRING	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment (A0) OR Non-Repudiation (40)		CA	M	C	OCTET STRING	

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
Signature		RSA signature with SHA-256		CA	M	n/a	BIT STRING	

4.4 eID 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 eID 3 CA vX • Pointsharp eID Mobile 3 CA vX • Pointsharp eID 2 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>	230312113230Z	n/a	UTCTime	

Attribute (OID)	Max length	Value	Example	Critical/Non-critical	Data type	Comments
Next Update	13	<This Update + 48 hours>	230314113230Z	n/a	UTCTime	
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 eID 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 eID 3 CA vX • Pointsharp eID Mobile 3 CA vX • Pointsharp eID 2 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>	230312113230Z		UTCTime	
notAfter	13	<notBefore + 3 months>	230612113230Z		UTCTime	
Subject				n/a		
commonName (2.5.4.3)	64	<CN of Issuing CA> OCSP Responder Z	Pointsharp eID 3 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 eID 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)		SecMaker eID Root CA v1			UTF8String
organizationName (2.5.4.10)		SecMaker 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 'SecMaker eID 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 eID 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)		SecMaker eID Root CA v1			UTF8String	
organizationName (2.5.4.10)		SecMaker 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>	230312113230Z		UTCTime	
notAfter	13	<notBefore + 1 year>	240312113230Z		UTCTime	
Subject				n/a		
commonName (2.5.4.3)	64	SecMaker eID Root CA v1 OCSP Responder Z	SecMaker eID Root CA v1 OCSP Responder 1		UTF8String	'Z' represents a digit for the instance number of the responder.
organizationName (2.5.4.10)	64	SecMaker 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 'SecMaker eID 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	

4.8 eID Admin Subscriber certificates - Individuals

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
Version	1	3		CA	M	n/a	Integer	
serialNumber	64	Randomized	7899f9a6128e29824c8bccf757f06f16	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)		Pointsharp eID 2 CA vX		CA	M		UTF8String	'X' in the CA names represents a digit for the CA version.
organizationName (2.5.4.10)		Pointsharp AB		CA	M		UTF8String	
countryName (2.5.4.6)		SE		CA	M		PrintableString	

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
Validity		minimum 1 day, maximum 5 years				n/a	n/a	
notBefore	13	<Subscriber certificate issuing date and time>	230301011030Z	CA	M		UTCTime	
notAfter	13	<notBefore + Validity>	280301011030Z	CA	M		UTCTime	
Subject						n/a		
serialNumber (2.5.4.5)	64		158503240001 OR 4711	RA	M		Printable String	Consists of '15' followed by the birthdate of the user <YYMMDD> and a four digit serial number. OR Subscriber PoSC ID

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
givenName (2.5.4.42)	64	<first name> Admin	Lena <Admin>	RA	M*		UTF8String	The first name of the subscriber followed by 'Admin' or another description choosen by the RA. * For individuals that have no given name only the description will be used.
surName (2.5.4.4)	64		Svensson	RA	M		UTF8String	The middle names and surnamn of the subscriber.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
commonName (2.5.4.3)	64		Lena <Admin> Svensson	RA	M		UTF8String	A 'friendly name' of the subscriber. The first name and surname of the subscriber.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
title (2.5.4.12)	64	<Subscriber PoSC ID>	4711	CA	O		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 normally included in the certificate but may be omitted.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
organizationName (2.5.4.10)	64		Organization X	CA	M		UTF8String	Official name of the RA organization.
organizationalUnitName (2.5.4.11)	128		SE556691063301 OR SEBOLREG.5566910633	CA	M		UTF8String	The VAT identification number of the RA organization if such exists, alternatively the EUID.
organizationalUnitName (2.5.4.11)	128		HR	RA	O		UTF8String	An organizational unit within the RA organization related to the subscriber.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
localityName (2.5.4.7)	128		Stockholm	CA	M		UTF8String	The main locality of the RA organization.
countryName (2.5.4.6)	2		SE	CA	M		Printable String	The country where the RA organization has its main business.
Cardnumber extension (1.2.752.34.2.1)	19	<CardNumber according to Swedish standard SS614331>		Card Supplier or CA	M	NC	Printable String	Hard and soft tokens not beeing "cards" will also be given a unique number in this extension.

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
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	
cRLDistributionPoints (2.5.29.31)		[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.pointsharpsecurecloud.com/pointsharpeid2cavX.crl		CA	M	NC	OCTET STRING	'X' in the CA names of the URLs represents a digit for the CA version.

	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=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://repository.pointsharpsecurecloud.com/pointsharpeid2cavX.cer		CA	M	NC	OCTET STRING	'X' in the CA names of the URLs represents a digit for the CA version.
subjectAltName (2.5.29.17)						NC		
userPrincipalName (1.3.6.1.4.1.311.20.2.3)	255		lensve@pointsharp.com OR lena.svensson@pointsharp.com	RA	M			For AD logon.

	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> [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.pointsharpsecurecloud.com	The OID of the Policy Identifier must be: 1.2.752.179.102.2.0.6 - LoA2: Undefined, Admin user	CA	M		OCTET STRING CPS Qualifier =IA5 string	OID depending on the LoA issuing process and the purpose.
enhancedKeyUsage					M	NC		
clientAuthentication (1.3.6.1.5.5.7.3.2)				CA	M			
smartCardLogon (1.3.6.1.4.1.311.20.2.2)				CA	M			

	Max length	Value	Example	Source	Mandatory/ Optional	Critical/ Non-critical	Data type	Comment
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	
subjectKeyIdentifier (2.5.29.14)						NC	n/a	
keyIdentifier		Hash of part of the subscriber's public key			M		OCTET STRING	
authorityKeyIdentifier						NC	n/a	
keyIdentifier		subjectKeyIdentifier of the Issuing CA. Hash of part of the Issuing CA's public key.		CA	M		OCTET STRING	
keyUsage (2.5.29.15)		digitalSignature, keyEncipherment (A0)		CA	M	C	OCTET STRING	
Signature		RSA signature with SHA-256		CA	M	n/a	BIT STRING	

POINTSHARP

Website
https://www.pointsharp.com

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

Classification:	Public
Publ. No.:	PSC-Rd21-02
Document version:	2.1
Document status:	Final
OID:	
Published:	24 Mar 2023