

7 Profiles

7.1 Certificate Profile

7.1.1 Basic Certificate Fields

X.509 Field name	X.509 Value	Comment
Version Number	Shall indicate that the version is 3.	
Serial Number	Unique Certificate Serial Number.	
Signature Algorithm	Object identifier of the algorithm used to sign the Certificate: sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}	
Issuer	CN=First ZebSign Community ID CA O=ZebSign - <ZebSign org.nr.> C=NO	
Validity	notBefore <UTCTime> notAfter <UTCTime>	2 or 3 years for Smart Card ID 2 years for Desktop ID
Subject	Community Personal ID: SerialNumber=<Distinguish ID>	Makes the subject unique (distinguished) within the Community.
	Community Subscriber Member ID: SerialNumber=<Employee Number>	
	CN=<First Name> <Middle Name> <Last Name>	
	OU=<Organzational Unit Name>	Optional field, specified by the Subscriber. Not used for Community Personal ID.
	O=<Subscriber Name> – <Subscriber Unique Identifier>	Not used for Community Personal ID.
	C=NO	
Subject Public	RSA–1024,	

Key Info	sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}	
----------	---	--

Table 1 Certificate basic fields

7.1.2 Certificate Extensions

All extensions are non-critical except for key usage.

X.509 Field name	X.509 Value	Mandatory / Optional / Conditional
Authority Key Identifier	The value is: 4D2E 1646 3FD2 6D20	M
Subject Key Identifier	Contains an 8 byte value	M
keyUsage	Certificate 1: nonRepudiation. Certificate 2: digitalSignature, keyEncipherment, dataEncipherment, keyAgreement	M
Certificate Policy	Contains CertPolicyId as specified in § 1.2 in this policy	M
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	M
cRL Distribution Points	Distribution Point Name, Full Name: URL= ldap://ldap.zesign.com/CN=First%20ZebSign%20Community%20ID%20CA,O=ZebSign%20-%20983163432,C=NO?certificateRevocationList?base URL= http://crl.zesign.com/crl/cid.crl	M
Authority Information Access	URI to OCSP Service: id-ad-ocsp: URL=http://ocsp.zesign.com/zebsign/ocsp/ URI to CA Certificate on web: id-ad-caIssuer: URL= http://ca.zesign.com/ca/cid.cer	M
Qualified Certificate Statements	Contains the following statement: esi4-qcStatement-1	M
subjectAlt Name	Several attributes are supported. Examples: rfc822Name= <E-mail address> OtherName, PrincipalName (1.3.6.1.4.1.311.20.2.3)	O
extKeyUsage	Several different settings are allowed. A few examples: Secure Email(1.3.6.1.5.5.7.3.4) Client Authentication(1.3.6.1.5.5.7.3.2) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Encrypting File System(1.3.6.1.4.1.311.10.3.4)	O
CardNumber	Smart Card Number extension according to Swedish standard SS 614331. Only included in Smart Card ID certificates.	C

Table 2 Certificate extensions

7.2 CRL Profile

ZebSign issues CRLs that conform to RFC 2459 [9].

Name	Mandatory	Description
Version	M	Version is set to v2
Signature	M	Defines the algorithm used to sign the CRL.
Issuer	M	The field shall contain the subject DN of the CA that issued the CRL
ThisUpdate	M	Specifies when the CRL was generated
Next Update	M	Specifies when the CRL expires. The next CRL shall be issued before the current CRL expires.
RevokedCertificates		
certSerialNumb	M	The serial number of the revoked Certificate
revocationDate	M	The date of revocation
Reason Code	M	Identifies the reason for revocation
CRL number	M	
Authority Key Identifier	M	Identifies the public key corresponding to the private key used to sign a revocation list.

After a grace period, expired Certificates are removed from the CRL.

7.2.1 Version numbers supported for CRLs

The version of CRLs shall be version 2.

7.2.2 CRL and CRL entry extensions populated and their criticality.

No stipulations.