

ZebSign Standard ID Certificate Profile

Version: 0.95

Status: Draft version for comments

Date: January 11. 2006

ZebSign AS
Haavard Martinsensvei 54
0045 Oslo

Tlf : 22 89 84 80
Fax: 22 89 84 88
e-post:zebsign@zebsign.no

Document maintenance

This document is based on CP v1.1 and updated by ZebSign PMB.

Document history

All changes in the document shall be identified here. A change shall be described with version number, date of change and a short text outlining the main issues that have been changed. Internal reviews are removed before publication.

Version	Date	Comments	Responsible	Approved by
0.95	Jan 2006		ZebSign PMB	ZebSign PMB
		Ready for external review.		

Table of Contents

1.	SCOPE AND PURPOSE	4
2.	REFERENCES	4
3.	CERTIFICATES	5
3.1	CA Certificates	5
3.1.1	Standard ID CA Certificate	5
3.2	Subscriber Certificates	6
3.2.1	Standard ID End User Signature Certificates	6
3.2.2	Standard ID End User Encryption Certificates	7
4.	CRL PROFILE	8

1. SCOPE AND PURPOSE

This document contains detailed information about the certificates used by ZebSign and partners. This information is considered too detailed to be of interest for readers of policy documents, and is therefore distributed in a separate document on a need-to-know basis. This document is not considered more sensitive than the rest of the policy documents.

The purpose of this document is to provide one single place for specification of certificate contents. This serves to avoid inconsistency and hopefully contributes to a significant reduction of the risk for errors and misunderstandings in the maintenance of certificate contents.

2. REFERENCES

Ref	Document
[1]	ZebSign Object Identifiers, current version – maintained by ZebSign PMB.
[2]	SEID-Prosjektet Leveranse oppgave 1 "Anbefalte sertifikatprofiler for personsertifikater og virksomhetssertifikater", versjon 1.01, 07.september 2004
[3]	RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[4]	ETSI TS 101 862 v1.3.1 (2004-03), Qualified Certificates Profile
[5]	ETSI TS 102 280 v1.1.1 (2004-03), X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

ZebSign PMB

3. CERTIFICATES

3.1 CA Certificates

All DirectoryString attributes in subject and issuer distinguished name are encoded using UTF8String.

3.1.1 Standard ID CA Certificate

This certificate is self-signed.

Section	Key	Value
Distinguished name	Country (C)	NO
	Organization (O)	ZebSign AS-983163432
	Common Name (CN)	ZebSign Standard ID CA 1
Attributes	Version	3
	Key type	RSA
	Key size	2048 bit
	Validity period	12 years
Extentions	Basic Constraints (critical)	Pathlength=0, CA=True
	Key Usage (critical)	KeyCertSign + CRLSign
	PolicyOID	2.16.578.1.9.10.2
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included.
Other	Signature algorithm	SHA-1 With RSA Encryption

Keystore: HSM

ZebSign PMB

3.2 Subscriber Certificates

All DirectoryString attributes in subject distinguished name are encoded using UTF8String.

3.2.1 Standard ID End User Signature Certificates

Section	Key	Value
Distinguished name	Country (C)	NO
	Organization (O)	Conditional: <Name of Organization>-<Org. No> ¹
	Organizational Unit (OU)	Optional: <Name of OU> ²
	Serial Number	<Unique ID> ³
	Common Name (CN)	<Commonly used name of subscriber>
Attributes	Version	3
	Key type	RSA
	Key size	1024 bit
	Validity period	Token: Maximum 3 years Desktop: Maximum 2 years
Extensions	Key Usage (critical)	NonRepudiation + DigitalSignature
	Authority Information Access	Access method = OCSP: URI = <URI to VA service> Access method = CA-Issuer: URI = <URI to CA-certificate>
	PolicyOID	Token: 2.16.578.1.9.7.1.1 Desktop: 2.16.578.1.9.7.1.3
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included.
	SubjectAltName	Supported Optional Attributes: - RFC822Mail = <e-mail address of the subject> - OtherName, Principalname = <Subject UPN>.
	Extended Key Usage	Optional Extension. Allowed values are: Client Authentication E-Mail Protection Smartcard Logon
	Card ID (private ext)	Token serialNumber. Only included in certificates stored on Token.
CRL Distribution Point	Optional Extension: URI = <URI to ldap service> URI = <URI to http service>	
Other	Signature algorithm	SHA-1 With RSA Encryption

Keystore: Token / Desktop

¹ Organization is mandatory for Standard Subscriber Member certificates. Organization is not permitted for Standard Personal certificates.

² Organizational Unit is optional for Standard Subscriber Member certificates. Organizational Unit is not permitted for Standard Personal certificates.

³ An alphanumeric value, which shall ensure that the DN is unique for human subjects, according to specification in [2].

ZebSign PMB

3.2.2 Standard ID End User Encryption Certificates

Section	Key	Value
Distinguished name	Country (C)	NO
	Organization (O)	Conditional: <Name of Organization>-<Org. No> ¹
	Organizational Unit (OU)	Optional: <Name of OU> ²
	Serial Number	<Unique ID> ³
	Common Name (CN)	<Commonly used name of subscriber>
Attributes	Version	3
	Key type	RSA
	Key size	1024 bit
	Validity period	Token: Maximum 3 years Desktop: Maximum 2 years
Extensions	Key Usage (critical)	KeyEncipherment + DataEncipherment
	Authority Information Access	Access method = OCSP: URI = <URI to VA service> Access method = CA-Issuer: URI = <URI to CA-certificate>
	PolicyOID	Token: 2.16.578.1.9.7.1.1 Desktop: 2.16.578.1.9.7.1.3
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included.
	SubjectAltName	Supported Optional Attributes: - RFC822Mail = <e-mail address of the subject> - OtherName, Principalname = <Subject UPN>.
	Extended Key Usage	Optional Extension. Allowed values are: E-Mail Protection Encrypted File System
	Card ID (private ext)	Token serialNumber. Only included in certificates stored on Token.
	CRL Distribution Point	Optional Extension: URI = <URI to ldap service> URI = <URI to http service>
Other	Signature algorithm	SHA-1 With RSA Encryption

Keystore: Token / Desktop

¹ Organization is mandatory for Standard Subscriber Member certificates. Organization is not permitted for Standard Personal certificates.

² Organizational Unit is optional for Standard Subscriber Member certificates. Organizational Unit is not permitted for Standard Personal certificates.

³ An alphanumeric value, which shall ensure that the DN is unique for human subjects, according to specification in [2].

4. CRL PROFILE

Name	Format	Description
Version	INTEGER	Version shall be v2, i.e. value 1
Signature	AlgorithmIdentifier	SHA-1 With RSA Encryption
Issuer	Name	The field shall contain the subject DN of the CA that issued the CRL
ThisUpdate	UTCTime	Specifies when the CRL was generated
NextUpdate	UTCTime	Specifies when the CRL expires. The next CRL shall be issued before the current CRL expires
RevokedCertificates		Optional if no certificates present
.certSerialNumb	INTEGER	The serial number of the revoked certificate
.revocationDate	UTCTime	The date of revocation
.crlEntryExtensions	Extensions	Optional: <ul style="list-style-type: none">• ReasonCode may be used• InvalidityData is not used
CrlExtensions	Extensions	<ul style="list-style-type: none">• AuthorityKeyIdentifier (with KeyID only)• CRLNumber• IssuingDistributionPoint (Optional)

Note that RevokedCertificates may be empty.

Expired certificates should be removed from the CRL.

For definition of EntryExtensions and CRLExtensions see RFC 3280 [3].

None of the Extensions are marked as critical.