ZealiD AB		Document name ZealiD OCSP Profile		
Owner CEO	Class P	Category Steering	Date 2020-10-06	Revision 08

ZealiD OCSP Profile

ZealiD

ZealiD AB		Document name ZealiD OCSP Profile		
Owner CEO	Class P	Category Steering	Date 2020-10-06	Revision 08

ZealiD AB		Document name ZealiD OCSP Profile		
Owner CEO	Class P	Category Steering	Date 2020-10-06	Revision 08

Revision History

Date	Revision	Comment	Contributor
2019-06-21	01	Re Formatting from other document	Philip Hallenborg
2019-06-21	02	Published	Philip Hallenborg
2019-07-01	03	Certificate profile	Tomas Zuoza
2019-07-15	04	Updating information	Ignas Karpiejus
2019-11-10	05	Rebranded	Tomas Zuoza
2019-12-15	06	Added specification of for which certificate this profile is for and updated it accordingly	Tomas Zuoza
2020-05-28	07	Updated document with a new format and filled in missing information	Tomas Zuoza
2020-10-06	08	Added “noCheck” extension to OCSP Profile	Tomas Zuoza

1. Introduction

The document describes the profiles of the digital certificates of ZealiD. This document complements ZealiD QeID Certificate Practice Statement.

2. Technical Profile of Certificate

Certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280, ETSI EN 319 412-2 and ETSI EN 319 411-2 (chapter 6).

2.1. Certificate Body

Field	Mandatory	Value	Description
Subject Name			
Country	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code [3])
Postcode	Yes	11156	Postal code
Address	Yes	Box 3437, Stockholm	Mailing address
Email	Yes	support@zealid.com	Contact email
Organisation	Yes	ZealiD AB	Organisation name
Common Name	Yes	ZealiD OCSP Issuing 2020, ZealiD OCSP 2020 Root	Certificate authority name: Issuing is used for signing status responses of Subscriber Certificates. Root is used for signing status responses of the issuingCA
Organization Identifier	Yes	SE5569724288	Identification of the organisation different from the organisation name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Issuer Name			
Country	Yes	SE	Country code: SE - Sweden (2 character ISO 3166 country code [3])

Postcode	Yes	11156	Issuer postal code
Address	Yes	Box 3437, Stockholm	Issuer mailing address
Email	Yes	support@zealid.com	Issuer contact email
Organisation	Yes	ZealiD AB	Issuer organisation name
Common Name	Yes	ZealiD Issuing CA 2020, ZeailD Root CA 2020	Certificate authority name: Issuing CA is used for Issuing OCSP. Root CA is used for Root OCSP.
Organization Identifier	Yes	SE5569724288	Identification of the issuer organisation different from the organisation name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Serial Number	Yes		Unique serial number of the certificate
Version	Yes	3	Certificate format version
Signature Algorithm	Yes	sha384WithRSAEncryption	Signature algorithm in accordance to RFC 5280
Not Before	Yes		First date of certificate validity.
Not After	Yes		The last date of certificate validity.
Public Key info			
Algorithm	Yes	RSA	RSA algorithm in accordance with RFC 4055]
Public Key	Yes		Public Key

Extensions			
Extension	Values and Limitations	Criticality	Mandatory
Key Usage	digitalSignature, nonRepudiation	Critical	Yes
Basic Constraints	Subject Type=End Entity	Critical	Yes
Extended Key Usage	ocspSigning	Non-critical	Yes
Subject Key Identifier	SHA-1 hash of the public key	Non-critical	Yes
Authority Key Identifier	SHA-1 hash of the public key	Non-critical	Yes
Certificate Policies	Policy ID #1 (0.4.0.2042.1.2) Qualifier ID #1 CPS (1.3.6.1.5.5.7.2.1) CPS URI https://www.zealid.com/repository	Non-critical	Yes
OCSP No Revocation Check	No check enabled	Non-critical	Yes, in Issuing CA OCSP

2.2. OCSP Response Profile

OCSP v1 according to [RFC 6960]

Field	Values and Limitations	Description
ResponseStatus	0 for successful or error code	Result of the query
ResponseType	id-pkix-ocsp-basic	Type of the response
Version	1	Version of the response format
Responder ID	byName: EMAIL = support@zealid.com CN = ZEALID OCSP Issuing 2020 or ZEALID OCSP 2020 Root OI= SE5569724288 O = ZealiD AB C = SE STREET = Box 3437, Stockholm postalCode = 11156	Distinguished name of the OCSP responder. CN of the responder is named according to the underlying certificate.
Produced At		Date when the OCSP response was signed
Responses		
CertID		Serial number of the certificate
Cert Status		Status of the certificate as follows: *good* - certificate is issued and has not been revoked *revoked* - certificate is revoked *unknown* - the issuer of certificate is unrecognized by this OCSP responder, not issued by this CA
Revocation Time		Date of revocation or expiration of certificate
Revocation Reason		Code for revocation Reason according to RFC 5280 [4]
This Update		Date when the status was queried from database

nextUpdate		Set to "99991231235959Z" when computing last OCSP response
ArchiveCutOff	15 years	Archive cutoff date after a certificate has expired
Signature Algorithm	sha256withRSAEncryption sha384withRSAEncryption	Signing algorithm pursuant to RFC 5280 [4]. Sha384 is used to sign Subscriber Signing and Authentication certificate status responses. Sha256 is used to sign issuingCA status responses.

*OCSP does not support using *nonce* extension.