ZealiD AB		Document name ZealiD TSA CA Profile		
Owner CEO	Class P	Category Steering	Date 2022-03-16	Revision 01

ZealiD TSA CA and TSU

Certificate Profile

ZealiD

ZealiD AB		Document name ZealiD TSA CA Profile		
Owner CEO	Class P	Category Steering	Date 2022-03-16	Revision 01

ZealiD AB		Document name ZealiD TSA CA Profile		
Owner CEO	Class P	Category Steering	Date 2022-03-16	Revision 01

Revision History

Date	**Revision**	**Comment**	**Contributor**
2022-03-16	01	New TSA Profile	Tomas Zuoza

1. Introduction

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

2. Technical Profile of Certificate

Certificate is compiled in accordance with the X.509 version 3, IETF RFC 3161, ETSI EN 319 421, and ETSI EN 319 422.

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 TSA CA 2022	Certificate authority name
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 Root CA 2020	Certificate authority name
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	keyCertSign, crlSign	Critical	Yes
Basic Constraints	Subject Type=CA, Path Length Constraint=0	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 Authority Information Access	Method #1 OCSP (1.3.6.1.5.5.7.48.1) URI https://ocsp.zealid.com	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 Qualifier ID #2 User Notice (1.3.6.1.5.5.7.2.2) User notice Certificate has been issued according to NCP+ policy	Non-critical	Yes

2.2. TSU Profile

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 TSU1	TSU name
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 TSA CA 2022	Certificate authority name

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	sha256WithRSAEncryption	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	Critical	Yes
Basic	Subject Type=End Entity	Critical	Yes

Constraints			
Extended Key Usage	Purpose: Time Stamping	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 Authority Information Access	Method #1 OCSP (1.3.6.1.5.5.7.48.1) URI https://ocsp.zealid.com	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 Qualifier ID #2 User Notice (1.3.6.1.5.5.7.2.2) User notice Certificate has been issued according to NCP+ policy	Non-critical	Yes