ZealiD Subscriber Certificate Profiles

ZealiD AB		Document name ZealiD Subscriber Certificate Profiles		
Owner CEO	Class P	Category Steering	Date 2020-05-28	Revision 07

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

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

Natural person 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. Signing Certificate Body

Field	Mandatory	Value	Description
Subject Name			
Country	Yes		Country code: 2 character ISO 3166 country code [3]
Common Name	Yes		Given Name, Surname and Serial Number of the Subscriber
Given Name	Yes		Given Name of the Subscriber
Surname	Yes		Surname of the Subscriber
Serial Number	Yes		Identification of the natural person different from the common name. Certificates may include one or more semantics identifiers as specified in clause 5.1.3 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	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	nonRepudiation	Critical	Yes
Basic Constraints	Subject Type=End Entity	Critical	Yes
Subject Key	SHA-1 hash of the public key	Non-critical	Yes

Identifier			
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 Method #2 calssuers (1.3.6.1.5.5.7.48.2) URI https://www.zealid.com/repository/ZealiD_Issuing_CA.der	Non-critical	Yes
Certificate Policies	Policy ID #1 (0.4.0.194112.1.2) 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 QCP-n-qscd policy Policy ID #2 (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
Qualified Certificate	- Qualified Certificate Compliance - Qualified Certificate Type: Type-1: Qualified	Non-critical	Yes

Statements	Certificate for Electronic Signatures - Private key resides in a QSCD - PKI Disclosure Statements (PDS): https://www.zealid.com/hubfs/ZealiD%20PKI%20Disclosure%20Statement%20v%203.pdf, lang=EN		

2.2. Authentication Certificate Body

Field	Mandatory	Value	Description
Subject Name			
Country	Yes		Country code: 2 character ISO 3166 country code [3]
Common Name	Yes		Given Name, Surname and Serial Number of the Subscriber
Given Name	Yes		Given Name of the Subscriber
Surname	Yes		Surname of the Subscriber
Serial Number	Yes		Identification of the natural person different from the common name. Certificates may include one or more semantics identifiers as specified in clause 5.1.3 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	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 Constraints	Subject Type=End Entity	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 Method #2 calssuers (1.3.6.1.5.5.7.48.2) URI https://www.zealid.com/repository/ZealiD_Issuing_CA.der	Non-critical	Yes
Certificate Policies	Policy ID #1 (0.4.0.194112.1.2) 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 QCP-n-qscd policy Policy ID #2 (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)	Non-critical	Yes

	User notice Certificate has been issued according to NCP+ policy		
Qualified Certificate Statements	- Qualified Certificate Compliance - Qualified Certificate Type: Type-1: Qualified Certificate for Electronic Signatures - Private key resides in a QSCD - PKI Disclosure Statements (PDS): https://www.zealid.com/hubfs/ZealiD%20PKI%20Disclosure%20Statement%20v%203.pdf, lang=EN	Non-critical	Yes