Certificate Profiles

Advanced Certificates

ZertES

(Datum: 22.06.2026)

Root CA-Certificate

Field	Critical	Value
Version		V3
serialNumber		4a001d778aa039bb1eb44456d0de6b1621d0e315
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier		RSA (1.2.840.113549.1.1.1)
Key Size		4096 Bits
Issuer		
countryName (2.5.4.6)		DE
State (2.5.4.8)		Bavaria
organizationName (2.5.4.10)		SIGN8 GmbH
Organizational UnitName (2.5.4.11)		SIGN8 GmbH ROOT CA 01
organizationIdentifier (2.5.4.97)		DE349977882
commonName (2.5.4.3)		SIGN8 GmbH ROOT CA 01
Validity		
NotBefore		28.04.2022 18:23:14
NotAfter		24.04.2037 18:23:14

Subject		
countryName (2.5.4.6)		DE
State (2.5.4.8)		Bavaria
organizationName (2.5.4.10)		SIGN8 GmbH
Organizational UnitName (2.5.4.11)		SIGN8 GmbH ROOT CA 01
organizationIdentifier (2.5.4.97)		DE349977882
commonName (2.5.4.3)		SIGN8 GmbH ROOT CA 01
Extensions		
KeyUsage (2.5.29.15)	✓	keyCertSign, cRLSign
basicConstraints (2.5.29.19)	✓	Subject is a CA Path Length Constraint: None
authorityKeyIdentifier (2.5.29.35)		63f07b0c0bb72741e887715176ee3d62e0fd9d94
subjectKeyIdentifier (2.5.29.14)		63f07b0c0bb72741e887715176ee3d62e0fd9d94

CA-Certificates

Field	Critical	Value
Version		V3
serialNumber		629D7A4480DCD113492E32517F46A000F658263C (SIGN8 CH ADVANCED SIGNATURE CA 01) OR 629D7A4480DCD113492E32517F46A000F658263D (SIGN8 CH ADVANCED SIGNATURE CA 02) OR 629D7A4480DCD113492E32517F46A000F658263E (SIGN8 CH ADVANCED SEAL CA 01) OR 629D7A4480DCD113492E32517F46A000F658263F (SIGN8 CH ADVANCED SEAL CA 02)
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier		RSA (1.2.840.113549.1.1.1)
Key Size		4096 Bits
Issuer		
countryName (2.5.4.6)		DE
State (2.5.4.8)		Bavaria
organizationName (2.5.4.10)		SIGN8 GmbH
Organizational UnitName (2.5.4.11)		SIGN8 GmbH ROOT CA 01
organizationIdentifier (2.5.4.97)		DE349977882

commonName (2.5.4.3)		SIGN8 GmbH ROOT CA 01
Validity		
NotBefore		16.03.2026
NotAfter		13.03.2036
Subject		
countryName (2.5.4.6)		CH
organizationName (2.5.4.10)		SIGN8 AG
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRCH-CHE-410.954.825
commonName (2.5.4.3)		SIGN8 CH ADVANCED SIGNATURE CA 01 OR SIGN8 CH ADVANCED SIGNATURE CA 02 OR SIGN8 CH ADVANCED SEAL CA 01 OR SIGN8 CH ADVANCED SEAL CA 02
Extensions		
KeyUsage (2.5.29.15)	✓	digitalSignature, cRLSign, keyCertSign
basicConstraints (2.5.29.19)	✓	Subject is a CA Path Length Constraint: 0
authorityKeyIdentifier (2.5.29.35)		63F07B0C0BB72741E887715176EE3D62E0FD9D94

subjectKeyIdentifier (2.5.29.14)		905F40B35C6A05C6A698F9BC453AF6EFAAA9B36F (SIGN8 CH ADVANCED SIGNATURE CA 01) OR AE213551D55D 03F9 E66C C0A2 BF25 B449 1AAB 2BE6 (SIGN8 CH ADVANCED SIGNATURE CA 02) OR D386 62C2 002C 216D D8AF DC90 C258 062A 3143 4232 (SIGN8 CH ADVANCED SEAL CA 01) OR 4713 6280 F605 94A9 B2A8 0E04 8C9F D3CA 8CD7 8C0D (SIGN8 CH ADVANCED SEAL CA 02)
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.63345.2.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.ch/trust

End-Entity Certificates for Signatures

Field	Critical	Value
Version		V3
serialNumber		[Serial Number]
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier		ECC (1.2.840.10045.2.1) OR RSA (1.2.840.113549.1.1.1)
Key Size		256 Bits (ECC) OR 521 Bits (ECC) OR 4096 Bits (RSA)
Issuer		
countryName (2.5.4.6)		CH
organizationName (2.5.4.10)		SIGN8 AG
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRCH-CHE-410.954.825
commonName (2.5.4.3)		SIGN8 CH ADVANCED SIGNATURE CA 01 OR SIGN8 CH ADVANCED SIGNATURE CA 02
Validity		
NotBefore		[Issue Date]
NotAfter		Up to 1.825 days

Subject		
commonName (2.5.4.3)		[Givenname and/or Surname] OR [Pseudonym]
Surname (2.5.4.4)		[Surname]
GivenName (2.5.4.42)		[Givenname]
Pseudonym (2.5.4.42)		[Pseudonym]
CountryName (2.5.4.6)		[Country]
SerialNumber (2.5.4.5)		Serial number assigned by SIGN8 OR Identifier assigned by a government or civil authority
OrganizationName (2.5.4.10)		[Organization]
Extensions		
keyUsage (2.5.29.15)	✓	nonrepudiation
basicConstraints (2.5.29.19)		Subject is not a CA Path Length Constraint: None
subjectKeyIdentifier (2.5.29.14)		[Subject Key Identifier]
authorityKeyIdentifier (2.5.29.35)		905F 40B3 5C6A 05C6 A698 F9BC 453A F6EF AAA9 B36F (SIGN8 CH ADVANCED SIGNATURE CA 01) OR AE21 3551 D55D 03F9 E66C C0A2 BF25 B449 1AAB 2BE6 (SIGN8 CH ADVANCED SIGNATURE CA 02)
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.63345.2.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.ch/trust [1] Certificate Policy: • Policy Identifier: NCP+ (0.4.0.2042.1.2)
AuthorityInfoAccess		[0]: • Access Method: CaIssuers (1.3.6.1.5.5.7.48.2) • Access Location: ○ URI: https://aia.object.sign8.eu/[...] [1]:

		• Access Method: OCSP (1.3.6.1.5.5.7.48.1) • Access Location: ○ URI: http://ocsp-q.sign8.eu

End-Entity Certificates for Seals

Field	Critical	Value
Version		V3
serialNumber		[Serial Number]
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier		ECC (1.2.840.10045.2.1) OR RSA (1.2.840.113549.1.1.1)
Key Size		256 Bits (ECC) OR 521 Bits (ECC) OR 4096 Bits (RSA)
Issuer		
countryName (2.5.4.6)		CH
organizationName (2.5.4.10)		SIGN8 AG
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRCH-CHE-410.954.825
commonName (2.5.4.3)		SIGN8 CH ADVANCED SEAL CA 01 OR SIGN8 CH ADVANCED SEAL CA 02
Validity		

NotBefore		[Issue Date]
NotAfter		Up to 1.825 days
Subject		
commonName (2.5.4.3)		[Organization]
CountryName (2.5.4.6)		[Country]
organizationName (2.5.4.10)		[Organization]
OrganizationUnitName (2.5.4.11)		[OrganizationUnitName]
organizationIdentifier (2.5.4.97)		[Organization Identifier]
Extensions		
keyUsage (2.5.29.15)	✓	nonrepudiation
basicConstraints (2.5.29.19)		Subject is not a CA Path Length Constraint: None
subjectKeyIdentifier (2.5.29.14)		[Subject Key Identifier]
authorityKeyIdentifier (2.5.29.35)		D386 62C2 002C 216D D8AF DC90 C258 062A 3143 4232 (SIGN8 CH ADVANCED SEAL CA 01) OR 4713 6280 F605 94A9 B2A8 0E04 8C9F D3CA 8CD7 8C0D (SIGN8 CH ADVANCED SEAL CA 02)
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.63345.2.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.ch/trust [1] Certificate Policy: • Policy Identifier: NCP+ (0.4.0.2042.1.2)

AuthorityInfoAccess		[0]:
		• Access Method: CaIssuers (1.3.6.1.5.5.7.48.2)
		• Access Location:
		  ○ URI: https://aia.object.sign8.eu/[...]
		[1]:
		• Access Method: OCSP (1.3.6.1.5.5.7.48.1)
		• Access Location:
		  ○ URI: http://ocsp-q.sign8.eu

OCSP Certificates

Field	Critical	Value
Version		V3
serialNumber		[Serial Number]
Signature Algorithm		sha512RSA (1.2.840.113549.1.1.13)
Signature Hash Algorithm		sha512 (2.16.840.1.101.3.4.2.3)
Algorithm Identifier		ECC (1.2.840.10045.2.1) OR RSA (1.2.840.113549.1.1.1)
Key Size		256 Bits (ECC) OR 521 Bits (ECC) OR 4096 Bits (RSA)
Issuer		
countryName (2.5.4.6)		CH
organizationName (2.5.4.10)		SIGN8 AG
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRCH-CHE-410.954.825
commonName (2.5.4.3)		SIGN8 CH ADVANCED SIGNATURE CA 01 OR SIGN8 CH ADVANCED SIGNATURE CA 02 OR SIGN8 CH ADVANCED SEAL CA 01 OR SIGN8 CH ADVANCED SEAL CA 02
Validity		

NotBefore		[Issue Date]
NotAfter		Up to 1.825 days
Subject		
commonName (2.5.4.3)		OCSP + [CA Name]
serialNumber (2.5.4.5)		[SerialNumber]
Extensions		
keyUsage (2.5.29.15)	✓	digitalSignature
extendedKeyUsage (2.5.29.37)		OCSPSigning
OCSP No-Check (1.3.6.1.5.5.7.48.1.5)		null
basicConstraints (2.5.29.19)		Subject is not a CA Path Length Constraint: None
subjectKeyIdentifier (2.5.29.14)		[Subject Key Identifier]
authorityKeyIdentifier (2.5.29.35)		905F 40B3 5C6A 05C6 A698 F9BC 453A F6EF AAA9 B36F (SIGN8 CH ADVANCED SIGNATURE CA 01) OR AE21 3551 D55D 03F9 E66C C0A2 BF25 B449 1AAB 2BE6 (SIGN8 CH ADVANCED SIGNATURE CA 02) OR D386 62C2 002C 216D D8AF DC90 C258 062A 3143 4232 (SIGN8 CH ADVANCED SEAL CA 01) OR 4713 6280 F605 94A9 B2A8 0E04 8C9F D3CA 8CD7 8C0D (SIGN8 CH ADVANCED SEAL CA 02)
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.63345.2.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.ch/trust

AuthorityInfoAccess		[0]: • Access Method: CaIssuers (1.3.6.1.5.5.7.48.2) • Access Location: ○ URI: https://aia.object.sign8.eu/[...]