Certificate Profiles

Advanced Certificates

ETSI

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		N/A
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		N/A
NotAfter		N/A

Subject		
countryName (2.5.4.6)		DE
organizationName (2.5.4.10)		SIGN8 GmbH
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRDE-DED2601V.HRB271573
commonName (2.5.4.3)		SIGN8 ADVANCED SIGNATURE CA 03
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)		N/A
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.58197.1.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.eu/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)		DE
organizationName (2.5.4.10)		SIGN8 GmbH
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRDE-DED2601V.HRB271573
commonName (2.5.4.3)		SIGN8 ADVANCED SIGNATURE CA 03 OR SIGN8 ADVANCED SIGNATURE CA 04
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)		N/A
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.58197.1.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.eu/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)		DE
organizationName (2.5.4.10)		SIGN8 GmbH
Organizational UnitName (2.5.4.11)		Trust Services
OrganizationIdentifier (2.5.4.97)		NTRDE-DED2601V.HRB271573
commonName (2.5.4.3)		SIGN8 ADVANCED SEAL CA 03 OR SIGN8 ADVANCED SEAL CA 04
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)		N/A
Certificate Policies (2.5.29.32)		[0] Certificate Policy: • Policy Identifier: 1.3.6.1.4.1.58197.1.4.0 • PKIX CPS Pointer Qualifier (1.3.6.1.5.5.7.2.1): ○ https://sign8.eu/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