Certificate Profiles

Qualified Certificates

eIDAS

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		629d7a4480dcd113492e32517f46a000f658262a (SIGN8 QES SIGNATURE CA 03) OR 629d7a4480dcd113492e32517f46a000f658262c (SIGN8 QES SIGNATURE CA 04) OR 629d7a4480dcd113492e32517f46a000f658262b (SIGN8 QES SEAL CA 03) OR 629d7a4480dcd113492e32517f46a000f658262d (SIGN8 QES SEAL CA 04)
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		02.07.2024
NotAfter		29.062039
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 QES 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)		B55A16ADE711A624DCB35AD7DFEA6B97FC1AF8D2 (SIGN8 QES SIGNATURE CA 03) OR 845E43F2EDE1E540C0038D23E97A0114CA3FA4FE (SIGN8 QES SIGNATURE CA 04) OR

		F7305DD59EEA37F42E2C0871F9B2BC874F596A7A (SIGN8 QES SEAL CA 03) OR CFD66673B4F2F136194C919D97F647CFF98B998F (SIGN8 QES SEAL CA 04)
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 – 2. Generation

Signature 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)		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 QES SIGNATURE CA 03 OR SIGN8 QES SIGNATURE CA 04

Validity		
NotBefore		[Issue Date]
NotAfter		Up to 1.825 days
Subject		
commonName (2.5.4.3)		[Givenname Surname]
Surname (2.5.4.4)		[Surname]
GivenName (2.5.4.42)		[Givenname]
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)		B55A16ADE711A624DCB35AD7DFEA6B97FC1AF8D2 (SIGN8 QES SIGNATURE CA 03) OR 845E43F2EDE1E540C0038D23E97A0114CA3FA4FE (SIGN8 QES SIGNATURE CA 04)
qcStatements (1.3.6.1.5.5.7.1.3)		• QcCompliance: 0.4.0.1862.1.1 • QcType: 0.4.0.1862.1.6.1 (eSig) • QcSSCD: 0.4.0.1862.1.4 • QcPDS: 0.4.0.1862.1.5

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: QcpNaturalQscd (0.4.0.194112.1.2)

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

Seal 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)		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 QES SEAL CA 03 OR SIGN8 QES 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)		F7305DD59EEA37F42E2C0871F9B2BC874F596A7A (SIGN8 QES SEAL CA 03) OR CFD66673B4F2F136194C919D97F647CFF98B998F (SIGN8 QES SEAL CA 04)
qcStatements (1.3.6.1.5.5.7.1.3)		• QcCompliance: 0.4.0.1862.1.1 • QcType: 0.4.0.1862.1.6.2 (eSeal) • QcSSCD: 0.4.0.1862.1.4 • QcPDS: 0.4.0.1862.1.5

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: QcpLegalQscd (0.4.0.194112.1.3)
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

Obsolete Profiles

End-Entity Certificates - 1. Generation „eIDAS 1.0“

Signature Certificates

Field	Critical	Value
Version		V3
serialNumber (2.5.4.5)		
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
State		Bavaria
organizationName (2.5.4.10)		SIGN8 GmbH
OrganizationalUnitName (2.5.4.11)		SIGN8 GmbH QES Sign CA 01 OR SIGN8 GmbH QES Sign CA 02

commonName (2.5.4.3)		SIGN8 GmbH QES Sign CA 01 OR SIGN8 GmbH QES Sign CA 02
Validity		
NotBefore		
NotAfter		Up to 1.825 days
Subject		
commonName (2.5.4.3)		[first_name last_name]
Extensions		
keyUsage (2.5.29.15)	✓	digitalSignature, 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)		A88C81808328EA8AC6A89BCB7216A9FFC595463A (SIGN8 GmbH QES Sign CA 01) OR 9C476029FD75C9A21C7B3004ED1EF3EB1E7F487E (SIGN8 GmbH QES Sign CA 02)
qcStatements (1.3.6.1.5.5.7.1.3)		QcCompliance= 0.4.0.1862.1.1 QcType= • 0.4.0.1862.1.6.1 (eSig) QcSSCD= 0.4.0.1862.1.4 QcPDS = 0.4.0.1862.1.5

Certificate Policies (2.5.29.32)	✓	policyIdentifier= 1.3.6.1.4.1.58197.1.0.0 (CPS) policyQualifier= https://sign8.eu/trust/
AuthorityInfoAccess		OID: calssuers; URI: https://sign8.eu/trust (1.3.6.1.5.5.7.48.2) OID:OCSP; URI: http://ocsp-q.sign8.eu (1.3.6.1.5.5.7.48.1)

Seal Certificates

Field	Critical	Example value
Version		V3
serialNumber (2.5.4.5)		
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
State		Bavaria
organizationName (2.5.4.10)		SIGN8 GmbH
OrganizationalUnitName (2.5.4.11)		SIGN8 GmbH QES Seal CA 01 OR SIGN8 GmbH QES Seal CA 02
commonName (2.5.4.3)		SIGN8 GmbH QES Seal CA 01 OR SIGN8 GmbH QES Seal CA 02

Validity		
NotBefore		
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 e.g. EUID]
Extensions		
keyUsage (2.5.29.15)	✓	digitalSignature, 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)		52616CE4E123038D40751D7D083176F1BCBFE424 (SIGN8 GmbH QES Seal CA 01) OR 6BD4C9892A421F8F5580D20F86D681FE90F4C597 (SIGN8 GmbH QES Seal CA 02)

qcStatements (1.3.6.1.5.5.7.1.3)		QcCompliance= 0.4.0.1862.1.1 QcType= • 0.4.0.1862.1.6.2 (eSeal) QcSSCD= 0.4.0.1862.1.4 QcPDS = 0.4.0.1862.1.5
Certificate Policies (2.5.29.32)		policyIdentifier= 1.3.6.1.4.1.58197.1.0.0 (CPS) policyQualifier= https://sign8.eu/trust/
AuthorityInfoAccess		OID: caIssuers; URI: https://sign8.eu/trust (1.3.6.1.5.5.7.48.2) OID:OCSP; URI: http://ocsp-q.sign.eu (1.3.6.1.5.5.7.48.1)

Additional Information

Subject Distinguished Name fields (givenName, surname, and commonName) are populated directly from the authenticated attributes provided by the Identity Provider. The consistency of the encoding is checked by the Registration Authority.