Zugelassene Signatur-Zertifikate

Für die Einlieferung des eBill-Formats (PDF-Datei mit eingebettetem Anhang) in die eBill-Infrastruktur sind folgende Zertifikate für die Signierung zugelassen:

- geregelte elektronische Signaturen
- qualifizierte Zeitstempel

Die Zertifikate von folgenden Herausgebern (Aufzählung abschliessend) können für das Signieren der PDF-Datei eingesetzt werden:

Qualifizierte Organisationszertifikate

Anbieter	Issuing CA*	Kontakt
Swisscom	Swisscom Diamant CA 4	STS.SalesSupport@swisscom.com
SwissSign	Zurzeit kein Angebot	sales@swisssign.com
QuoVadis	QuoVadis Swiss Regulated CA G2x	qv.support.ch@digicert.com
	QuoVadis Swiss Regulated CA G3	
BIT	Swiss Government Regulated CA 02	pki-info@bit.admin.ch

*Beispiele; keine abschliessende Aufzählung

Qualifizierte Zeitstempel

Anbieter	Issuing CA*	Kontakt
Swisscom	Swisscom TSS CA 4.1	STS.SalesSupport@swisscom.com
SwissSign	SwissSign Qualified TSA ICA 2021 – 1	sales@swisssign.com Vermerk: Zertifikate SIX eBill
	SwissSign RSA SIGN ZertES Qualified TSA ICA 2023 – 1	
QuoVadis	QuoVadis Time-Stamping Authority CA G1	ch.support@digicert.com
BIT	Swiss Government Regulated CA 02	pki-info@bit.admin.ch

*Beispiele; keine abschliessende Aufzählung

Client-Authentisierung an Webservern – Zugelassene Authentisierungs-Zertifikate

Für den Zugriff auf die eBill & DD Plattform sind zwingend Client-Zertifikate einzusetzen.

SIX akzeptiert Client-Zertifikate verschiedenster Herausgeber (Certificate Authorities):

Anbieter	Issuing CA*	Kontakt
SwissSign	SwissSign RSA TLS DV ICA 2022 – 1 SwissSign RSA TLS EV ICA 2022 - 1 SwissSign RSA TLS OV ICA 2022 - 1 SwissSign RSA SMIME SV ICA 2024 - 1	sales@swisssign.com Vermerk: Zertifikate SIX eBill
QuoVadis / DigiCert	QuoVadis Swiss Advanced CA G4 QuoVadis Global SSL ICA G3 QuoVadis Global SSL ICA G2 DigiCert SHA2 Secure Server CA RapidSSL RSA CA 2018 DigiCert SHA2 Assured ID CA DigiCert SHA2 Extended Validation Server CA Thawte TLS RSA CA G1	ch.support@digicert.com

*Beispiele; keine abschliessende Aufzählung

Unternehmen, die Zertifikate anderer Drittanbieter verwenden wollen, nehmen vorgängig mit SIX Kontakt auf. Um eine hohe Sicherheit gewährleisten zu können, müssen die Zertifikate mindestens folgende Voraussetzungen erfüllen:

- Gültigkeit der Benutzer-Zertifikate: nicht abgelaufen, bei Neuanmeldung noch neun Monate gültig
- Gültigkeit der Root-Zertifikate: nicht abgelaufen, bei Neuanmeldung noch fünf Jahre gültig
- Standard: X.509 V3
- Signaturalgorithmus: sha2RSA
- Schlüssellänge: mind. 2048 Bit
- Key Usage: Client Authentication, digital Signature