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	Swisscom	SwissSign	QuoVadis	BIT
Issuing CA*	Swisscom Diamant CA 4	Zurzeit kein Angebot	QuoVadis Swiss Regulated CA G2x QuoVadis Swiss Regulated CA G3	Swiss Government Regulated CA 02

*Beispiele; keine abschliessende Aufzählung

Qualifizierte Zeitstempel

Anbieter	Swisscom	SwissSign	QuoVadis	BIT
Issuing CA*	Swisscom TSS CA 4.1	SwissSign Qualified TSA ICA 2021 - 1 SwissSign TSA Platinum CA 2017 – G22	QuoVadis Time-Stamping Authority CA G1	Swiss Government Regulated CA 02

*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	DigiCert	SwissSign	QuoVadis
Issuing CA	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	SwissSign Personal Gold CA 2008 - G2 SwissSign Personal Gold CA 2014 - G22 SwissSign EV Gold CA 2014 - G22 SwissSign RSA TLS Root CA 2021 - 1 SwissSign RSA TLS EV ICA 2021 - 1	QuoVadis Swiss Advanced CA G4 QuoVadis Global SSL ICA G3 QuoVadis Global SSL ICA G2

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