Certificats de signature approuvés

En soumettant l'eBill bien formatée (fichier PDF avec pièce jointe intégrée) dans l'infrastructure eBill, les certificats suivants sont autorisés pour la signature électronique:

- signatures électroniques qualifiées
- horodatages qualifiés

Les certificats des fournisseurs suivants (liste exhaustive) peuvent être utilisés pour la signature du fichier PDF:

Certificats d'organisation qualifiés

Fournisseur	Issuing CA*	Contact
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

* Exemple seulement; liste non exhaustive

Horodatages qualifiés

Fournisseur	Issuing CA*	Contact
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

* Exemple seulement; liste non exhaustive

Authentification client sur les serveurs web – certificats d'authentification approuvés

Pour l'accès à la plateforme eBill & DD, il est impératif d'utiliser des certificats clients.

SIX accepte les certificats clients de plusieurs fournisseurs (autorités de certification):

Fournisseur	Issuing CA*	Contact
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

* Exemple seulement; liste non exhaustive

Les entreprises qui veulent utiliser les certificats de fournisseurs tiers ou des certificats propres à la banque, doivent au préalable prendre contact avec SIX. Afin de garantir un niveau sécurité élevé, les certificats doivent remplir au moins les conditions suivantes:

- Validité des certificats utilisateurs: n'a pas expiré, en cas de nouvelle inscription, est valable encore neuf mois
- Validité des certificats racine: n'a pas expiré, en cas de nouvelle inscription, est valable encore cinq ans
- Standard: X.509 V3
- Algorithme de signature: sha2RSA
- Longueur de clé: au min. 2048 bits
- Utilisation de la clé: authentification client, signature numérique