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	Swisscom	SwissSign	QuoVadis	BIT
Issuing CA*	Swisscom Diamant CA 4	Aucune offre pour le moment	QuoVadis Swiss Regulated CA G2x QuoVadis Swiss Regulated CA G3	Swiss Government Regulated CA 02

* Exemple seulement; liste non exhaustive

Horodatages qualifiés[1]

Fournisseur	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

* Exemple seulement; liste non exhaustive

[1] Déploiement possible dès avril 2022

Authentification client sur les serveurs web – certificats d'authentification approuvés[2]

Les certificats clients doivent être impérativement utilisés par les banques pour accéder à la plate-forme eBill & DD.

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

Fournisseur	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 G3 QuoVadis Global SSL ICA G3 QuoVadis Global SSL ICA G2

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

[2] Déploiement possible dès avril 2022; obligatoire à partir d'octobre 2022