Approved signature certificates

When submitting a properly formatted eBill (PDF file with embedded attachment) to the eBill infrastructure, the following certificates are permitted for digital signatures:

- qualified electronic signatures
- qualified time stamps

Certificates issued by the following providers (exhaustive list) can be used for signing the PDF file:

Qualified Organizational Certificates

Issuer	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

* Example only; not an exhaustive list

Qualified Timestamps

Issuer	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

* Example only; not an exhaustive list

Client certificates for web server authentication - approved authentication certificates

Client certificates must be used to access the eBill & DD platform.

SIX accepts client certificates from several issuers (certificate authorities):

Issuer	Issuing CA*	Contact
SwissSign	SwissSign RSA TLS DV ICA 2022 – 1	sales@swisssign.com Vermerk: Zertifikate SIX eBill
	SwissSign RSA TLS EV ICA 2022 - 1	
	SwissSign RSA TLS OV ICA 2022 - 1	
	SwissSign RSA SMIME SV ICA 2024 - 1	
QuoVadis / DigiCert	QuoVadis Swiss Advanced CA G4	ch.support@digicert.com
	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	
*Beispiele; keine abschliessende Aufzählung		

Companies that intend to use either certificates from other third-party providers or the bank's own certificates should contact SIX in advance. In order to guarantee a high level of security, the certificates must meet the following conditions at a minimum:

- Validity of the user certificate: not expired; new applications must be valid for another nine months
- Validity of the root certificate: not expired; new applications must be valid for another five years
- Standard: X.509 V3
- Signature algorithm: sha2RSA
- Key length: at least 2048 bit
- Key usage: client authentication, digital signature