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	Swisscom	SwissSign	QuoVadis	BIT
Issuing CA*	Swisscom Diamant CA 4	No offering at the moment	QuoVadis Swiss Regulated CA G2x QuoVadis Swiss Regulated CA G3	Swiss Government Regulated CA 02

* Example only; not an exhaustive list

Qualified Timestamps

Issuer	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

* Example only; not an exhaustive list

Client certificates for web server authentication - approved authentication certificates

Banks must use client certificates when accessing the eBill and DD platform.

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

Issuer	DigiCert	SwissSign	QuoVadis
Issuing CA	DigiCert SHA2 Secure Server CA	SwissSign Personal Gold CA 2008 - G2	QuoVadis Swiss Advanced CA G4
	RapidSSL RSA CA 2018	SwissSign Personal Gold CA 2014 - G22	QuoVadis Global SSL ICA G3
	DigiCert SHA2 Assured ID CA	SwissSign EV Gold CA 2014 - G22	QuoVadis Global SSL ICA G2
	DigiCert SHA2 Extended Validation Server CA	SwissSign RSA TLS Root CA 2021 - 1	
	Thawte TLS RSA CA G1	SwissSign RSA TLS EV ICA 2021 - 1	

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