eSignR
according to swiss/eu laws

Whitepaper

The Digital Signature: „An Enabler of Digital Transformation“

Administrative processes in the home office

During the Covid-19 lockdown, many companies became painfully aware that their administrative processes were not digitised at all or only partially. Anyone sitting in a home office who needs access to relevant documents would be happy to have an electronic filing system. But electronic filing alone is not enough when it comes to signing contracts with customers and business partners.

Many companies still rely on hand signatures for relevant documents such as contracts. If the signature rules in the company do not provide for individual signatures in certain cases, the signature round in the home office becomes a laborious undertaking. For example, if one of the contracting parties does not accept facsimile signatures (scan of hand signature), electronically available documents have to be printed out, signed by hand and circulated by post.

The digital signature is a factor that can simplify and accelerate the digital transformation of administrative processes.

What is the digital signature?

The electronic signature is a cryptographic (i.e. mathematical) procedure that makes possible the non-repudiable authorship and integrity of a document. The procedure works with a pair of keys. A secret signature key (private key) and a public verification key (public key). The originator of a document signs the document with his secret signature key. In the process, a value is calculated (the digital signature), which the recipient of the document can verify with the author‘s public verification key. The assignment of a certain key pair to a concrete person is done by a so-called digital certificate. Via the certificate, an existing signature can this be assigned to a person without any doubt. A signed document cannot be subsequently changed without the signature losing its validity.

The position of the digital digital signature in the law

The Swiss Federal Law on Electronic Signatures (ZertES) regulates how signature and verification keys must be used and managed by trusted third parties. These so-called providers of certification services must be recognised in accordance with ZertES in order for their products to have the desired legal effect.

The key pairs issued by the certification service providers can be used to apply so-called qualified electronic signatures to documents. According to the Swiss Code of Obligations (OR Art. 14 para. 2 bis), such signatures are equivalent to hand signatures.

In cross-border business transactions, it must be taken into account that there is currently no mutual recognition of digital signatures between Switzerland, the EU and other countries. In this case, a contract should sensibly bear digital signatures of the country whose law is applied and where the place of jurisdiction is.

What do I need for a digital signature?

To digitally sign, I need:

1) A certificate issued by a recognized certification service provider (i.e. a key pair).
2) Software to convert documents to PDF format.
3) A signature software to sign a PDF document with a personal secret signature key.

There are five recognized providers of certification services in Switzerland. They are Swisscom, QuoVadis, SwissSign, Swiss Government PKI (provider of certification services for the federal administration) and UBS (the bank!).

For the public, only Swisscom and QuoVadis issue certificates at the moment. Digital signatures are usually applied to documents that are in PDF format, the «digital paper».

Swisscom currently only offers certificates in conjunction with its own signature services. Such as Skribble (www.skribble.com). However, since this software requires documents to be uploaded in order to apply the signature, it is not possible to use the to be uploaded, using it for confidential documents is probably a no-go for many.

How can I verify the signature on a document?

Whether a signed document is «valid» cannot be answered by checking cryptographic properties alone. Rather, the context of the document must be taken into account:

- A signed contract between two companies is only valid if all signatures affixed to it are equivalent to hand signatures according to the law. In addition, the persons signing must be authorized to sign for the companies according to the commercial register entry and must have signed in accordance with the signature regulations (single signature, signature in twos).
- A digital criminal record extract is only valid if the only signature affixed to it is the signature of the person responsible for the criminal record, which is equivalent to a hand signature.
- An electronic document is only valid if it bears the signature of a person authorized by law to issue documents, such as a notary public, which is equivalent to a hand signature.

Since signatures are mainly applied to PDF documents, the PDF viewers of various manufacturers have implemented corresponding functions for checking signatures.

Examples include Adobe Acrobat Reader and Foxit Reader. All these programs are capable of performing the cryptographic (i.e. mathematical) checks of signatures, but fail to take into account the aspects listed above.

In order to perform not only the cryptographic but also the context-based verification of signatures, we have developed the Signature Validator (www.validator.ch) on behalf of the Federal Administration. The Validator supports the verification of signatures because it is able to include the context. The Validator is a web application into which one has to upload the document to be verified.

However, for confidential documents, this is probably a no-go for many. For this reason, the legally valid signature software Open eGov LocalSigner developed by us offers the possibility to validate signatures «discreetly», i.e. users do not have to upload documents to a cloud provider.

From Q1 2021 a brand new LocalSigner «eSignR» will be available. However, until eSignR is fully developed, we recommend using the Open eGov LocalSigner signature software we developed on behalf of the federal administration. LocalSigner is offered free of charge for Windows, macOS and Linux and can be downloaded here:

www.openegov.ch/localsigner

More information about eSignR at:
www.esignr.ch