

## Digital Signature

A digital signature is a technical equivalent of the hand-written signature. It is used to secure digital information, e.g. electronic documents. It is electronic data attached to the electronic document being signed, which identifies its author (the person signing it). Based on the aforementioned feature, the documents signed electronically can be made equal to paper documents.

The advantage of the digital signature lies in the fact that it is always unique, since it is a unique combination of characters created by means of a mathematical procedure and encoding. The digital signature differs also in being dependent on the content of the digital document, which is being signed. It means that if any change in the content of the signed document occurred, i.e. by interference of a third person or by the breakdown during its transmission through Internet, the recipient of the signed document will see it immediately during verification of the digital signature, therefore s/he will become aware of the infringement of the signed document.

We can ensure by means of the digital signature:

**Document authenticity** – it confirms that the person, who has signed the document digitally, is the person whom s/he claims to be. Recognition and unambiguous identification of a person signing the document is concerned. It means that the person, who this document is intended for, is sure that the person who signed the document digitally is really the persons s/he claims to be.

**Document integrity** - the message integrity ensures that the recipient received the document unchanged, i.e. that the document content has not been changed or forged after it has been signed digitally.

**Non-repudiation** – it helps all parties confirm the origin of the signed content. Non-repudiation means that the person who has signed the document digitally cannot reject the connection between the signed content and themselves, i.e. assert that the signature is not his/hers and that it was not him/her who has signed and sent the document in question.

For these guarantees to be affirmed it is necessary that the content was signed digitally by its author using the signature meeting the following criteria:

- The digital signature must be valid,
- The certificate assigned to the digital signature must be up-to-date (its validity has not expired yet),
- The signing organization denoting itself as the issuer, is trustworthy,

- The certificate assigned to the digital signature has been issued to the signing issuer by a trustworthy certificate authority.

The VÚB statements contain the digital signature issued by the VÚB certificate authority. Therefore, when opening the document, information that Acrobat reader does not recognize this certificate (the authority), is displayed to the clients. For it to be displayed correctly, the VÚB certificate needs to be imported (just once). The detailed procedure can be found on <http://www.vub.sk/files/osobne-financie/nonstop-banking/internet-banking/overenie-elektronickeho-podpisu-v-ar.pdf>.

You can find more information about the VÚB certificate authority at the webpage <https://registracia.vub.sk/pki/index.html>