

**Attitude to Article 17(2) of the Act No. 215/2002 Coll. on Electronic signature and on the amendment and supplementing of certain acts as amended  
(hereinafter referred to as the Act)**

Electronic signatures should enable also the communication going beyond the frontiers. This purpose requires to ensure that the Slovak electronic signatures are internationally valid and vice versa and lay down conditions under which the electronic signatures verified by a certification authority which was not accredited in Slovakia (hereinafter referred to as foreign electronic signatures) shall be recognized in the Slovak Republic.

Pursuant to Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (hereinafter referred to as the EU Directive) each state stipulates the conditions for validity of foreign electronic signatures on its territory; the EU Directive gives just recommendations.

The Act on Electronic signature in Article 17(2) (Recognition of certificates issued by CA being accredited abroad) amends this fact as follows: *“On the day of the Slovak Republic accession to the European Union, a certificate issued by the certification authority with its registered office in any Member State of the European Union, **whose validity can be verified in the Slovak Republic**, shall become equal to a certificate issued in the Slovak Republic. The qualified certificate issued by the given certification authority shall have the equal legal force and effect as the qualified certificate issued in the Slovak Republic.”*

In order to verify the qualified electronic signature issued by a foreign accredited certification authority, the capability to verify the validity of the certificate of a relevant public key is the decisive factor.

The process for the qualified electronic signature verification in the Slovak Republic is subject to legal regulations of the Slovak Republic and regardless of the fact that the qualified certificate is issued by a national or a foreign certification authority, the verification process must be identical in both cases. However, finally the both have the identical validity and identical legal effect in the Slovak Republic.

A verifier verifies the qualified electronic signature by means for the electronic signature verification using the signed electronic document and the public key belonging to a signatory. The qualified electronic signature verification means the verification whether the qualified electronic signature meets the formal requirements (approved formats of documents and signatures) and whether it is valid. Pursuant to Article 5(4) of the Act *“while verifying the qualified electronic signature the verifier shall on the basis of the qualified certificate of the public key verify whether the public key for the qualified electronic signature verification belongs to the signatory.”*

Procedure for the qualified electronic signature verification is regulated by the Decree of the National Security Authority No. 135/2009 Coll. on the creation and verification of the electronic signature and time stamp (hereinafter referred to as the Decree).

Pursuant to Article 11(5) of the Decree *“the verifier shall use the following to verify the validity of the qualified electronic signature*

- a) the electronic document for which the qualified electronic signature was created,*
- b) the qualified electronic signature of the electronic document,*
- c) the public key from a valid qualified certificate corresponding to the private key, by means of which the qualified electronic signature was created,*
- d) the signature policy in which the object identifier is specified in the qualified electronic signature or the valid object identifier of the accepted signature policy from the index pursuant to Art. 4(7),*
- e) the valid public keys corresponding to the private keys, by means of which the signatures of the certificates and certificate indexes were created in the certification path,*

*f) the certificate revocation lists for all certificates in the certification path, potential information on the status of certificates in the certification path obtained from the confirmation of the existence and validity of the certificate.*“

The qualified electronic signature verification requires the availability and completeness of information which are necessary and essential for the verification pursuant to the Act and decrees. Pursuant to the Decree the completeness of information means to attach to the qualified electronic signature *“complete information on all certificates of public keys needed for the verification of validity of the given qualified electronic signature, as well as the complete information on the certificate revocation lists or information on the status of the certificates which are decisive in the verification of the validity of the given qualified electronic signature.*“ Thus, for the verification of the qualified electronic signature validity it is not sufficient to verify only the public key of the signatory of the document.

From the mentioned above follows that in order to verify the qualified electronic signature validity trustworthily and securely in the Slovak Republic, it is required to know all the information about the qualified certificate of the signatory’s public key, all the information about the certificate of the accredited certification authority and all the information about the certificate of the National Security Authority. It is necessary to know the whole chain of certificates of the public key: *the qualified certificate of the signatory’s public key – the certificate of the public key of the accredited certification authority - the certificate of the public key of the National Security Authority.* The qualified certificate for the user must be issued by a credible institution / an accredited certification authority and therefore the knowledge of the certificate of the public key of the accredited certification authority is essential for the signature verification. This is not the end of the verification chain because in the hierarchy of the Public Key Infrastructure (PKI) the Root Certification Authority of the National Security Authority is superior to the accredited certification authority and therefore it is also necessary to verify the certificate of the public key of the National Security Authority, i.e. the certificate which is guaranteed by the state. If any of these certificates was not valid or revoked and listed in the Certificate Revocation List, it would not be possible to consider the signature being verified as trustworthy and it would not be possible to rely on its validity in legal acts.

#### The validity of the qualified certificate is verified by following methods:

1. Control of the validity of the user’s qualified certificate according to time data indicated in the certificate body by a certificate issuer, i.e. the accredited certification authority (validity from - to),
2. Control of potential early revocation of the user’s qualified certificate at the Certificate Revocation List (CRL) being issued by the certificate issuer (the accredited certification authority),
3. Control of authenticity of the user’s qualified certificate, i.e. control of the certificate signature, thus whether the certificate was issued by a trustworthy provider – the accredited certification authority.

#### The certificate validity of the accredited certification authority is verified by following methods:

1. Control of the certificate validity of the accredited certification authority according to time data indicated in the certificate body by a certificate issuer, i.e. the National Security Authority (validity from – to),

2. Control of potential early revocation of the certificate of the accredited certification authority at the Certificate Revocation List (CRL) being issued by the certificate issuer (the National Security Authority),
3. Control of authenticity of the certificate of the accredited certification authority, i.e. control of the certificate signature, thus whether the certificate was issued by the National Security Authority.

The certificate validity of the National Security Authority is verified by following methods:

1. Control of the certificate validity of the National Security Authority according to time data indicated in the certificate body by a certificate user, i.e. the National Security Authority (validity from – to),
2. Control of potential early revocation of the certificate of the National Security Authority at the Certificate Revocation List (CRL) being issued by the certificate issuer (the National Security Authority),
3. Control of authenticity of the certificate of the National Security Authority, i.e. control of the certificate signature, thus whether the certificate was issued by the National Security Authority. For that reason the public key of the National Security Authority is available directly at the National Security Authority and at the same time it is published in several information sources as laid down by the Act.

The National Security Authority is the certification authority of the highest level - so called the Root Certification Authority (RCA) in the Slovak Republic; therefore the verification process of the qualified electronic signature must always end up by the verification of the public key certificate of the National Security Authority.

The whole chain of the qualified certificate verification of the public key beginning with the qualified certificate of the signatory's public key and ending with the certificate of the Root Certification Authority's public key must be respected and preserved also in case of foreign certificates.

The National Security Authority pursuant to Article 34 of the Act No. 575/2001 Coll. on Organization of Activities of the Government and Organization of the Central State Administration, is the central body of the state administration for the electronic signature and thus a guarantor which performs the supervision of meeting the Act and its implementing regulations, what means it is a guarantee of the security of the electronic signature environment. The National Security Authority cannot be liable for foreign accredited certification authorities and their qualified certificates due to lack of right to supervision and unknown legislative, technical, organizational, security and other conditions under which these authorities provide their services.

The only feasible solution how to recognize the validity of the foreign qualified certificate in the Slovak Republic is to conclude an international agreement or to adopt the legislation within the European Union which shall bind each Member State to respect the comparable rules and accreditation procedures for the evaluation of the certification service provider trustworthiness (accredited certification authorities). The reciprocity of the qualified certificate recognition is also covered by this solution. Potential recognition of the foreign qualified certificate without meeting the above mentioned conditions would cause an inequality in the electronic signature environment, because all requirements of the Act would be possible to be enforced upon national accredited certification authorities, and only a few regulations upon the foreign certification authorities.

Within the European Union the evaluation process of the accredited certification authority credibility is ensured by the Commission Decision 2009/767/EC of 16 October 2009 which is setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. By that day an obligation has been imposed on public bodies to recognize qualified certificates issued by certification service providers of EU Member States provided that the relevant Member State shall publish the list of trustworthy service providers – Trusted List (TL).

Finally, it is important to emphasize again that in order to verify trustworthily the validity of the foreign qualified certificate, it is necessary that:

*a) the accredited certification authority from the EU Member State has been listed in the list of trustworthy service providers of relevant Member State,*

*b) an international agreement has been concluded between the Slovak Republic and the relevant state (the state which is not a Member State of the European Union; at present the Slovak Republic is not bound by such contract with any state), in which both states after the comparison of relevant legal norms and accreditation schemes shall be bound reciprocally by a contract about mutual recognition of issued qualified certificates.*