Promulgated: 18 October 2016. Version promulgated in the Collection of Laws of the Slovak Republic Time version of the Act effective since 01 August 2019.
The contents hereof are legally binding.

COLLECTIONS OF LAWS

OF THE SLOVAK REPUBLIC

2016

272

ACT

of 20 September 2016

on Trust Services for Electronic Transactions in the Internal Market and amendment of certain acts (Trust Services Act)

The National Council of the Slovak Republic adopted the following Act:

Article I

§1

Purpose of the Act

This Act stipulates the conditions for providing trust services,[1]) the obligations of trust service providers,[2]) the activities of the National Security Authority ("Authority") in the area of trust services and sanctions for violations of obligations under a special regulation[3]) and this Act.

§2

Usage of qualified electronic signature and qualified electronic seal in dealings with public authorities

(1) If qualified electronic signature[4]) or qualified certificate for electronic signature[5]) issued by a qualified trust service provider,[6]) to which the Authority conferred qualified status[7]) is used in dealings with public authorities, it may contain the birth number[9] of the signer as the specific attribute;[8]) if no birth number has been assigned, it may contain a passport number or identification card number.

(2) If a qualified electronic seal[10]) or qualified certificate for an electronic seal[11]) issued by a qualified trust service provider to which the Authority conferred qualified status is used in dealings with public authorities, the specific attribute[12]) it contains may be the identification number of the originator of the seal.[13])

Qualified trust service provider

§3

(1) A trust service provider without qualified status shall file notice of intent to provide qualified trust services[14]) to the Authority using the electronic form or in writing using the template published by the Authority on the central public administration portal and on its website. To the notice of intent to provide qualified trust services, the applicant shall attach certificates for the specific qualified trust services[15]) to be added to the trusted list[16]) after qualified status is conferred.

(2) A qualified trust service provider only provides qualified trust services for which it was conferred qualified status.

(3) A qualified trust service provider to which the Authority conferred qualified status for its trust services, shall disclose at a minimum the certification policy identifiers for qualified trust services of issuing the qualified certificate,[17]) which the Authority publishes on its website; certification policies also contain technical specifications and procedures for the signer and the originator of the seal.

§4

(1) A qualified trust service provider may authorise another internal qualified trust service or qualified trust service of another qualified trust service provider to provide information on the validity or revocation status of qualified certificates[18]) it issued. Information concerning authorisation per the first sentence above is disclosed in the trusted list maintained by the Authority. Authorisation is valid until revoked by the authorising qualified trust service provider or until the trust service loses qualified status.

(2) A qualified trust service provider may conclude an agreement with another qualified trust service provider if it terminates providing its qualified trust service; such agreement shall cover provisioning of information on the validity or revocation status of qualified certificates[18]) and the acceptance of related operational documentation. If a qualified trust service provider does not conclude an agreement per the first sentence and has no legal successor, the Authority shall provide information on the validity or revocation status of issued qualified certificates and the acceptance of related operational documentation. In the instances per the second sentence above, valid qualified certificates are cancelled upon acceptance by a qualified trust service provider, or, by the Authority upon acceptance in the database of certificates if the previous step is technically not feasible. Information concerning the procedure identified herein is disclosed in the trusted list maintained by the Authority.

§5

Qualified trust service providers shall archive information[19]) for a period of at least ten years

a) that is related to issuing and revoking qualified certificates from the expiry or revocation of the qualified certificate together with the issued qualified certificate and information on the validity or revocation status of a qualified certificate updated after expiry or revocation of the qualified certificate[18])

b) based on which it provided the qualified trust service; the qualified trust service provider shall archive such information from its inception.

§6

(1) Qualified trust service providers shall report details of any changes in their qualified trust services to the Authority at least 30 days before the planned change.

(2) Qualified trust service providers to which the Authority has conferred qualified status shall send the following to the Authority

a) issued qualified certificates for qualified electronic signature and qualified electronic seal within 30 days from issue of the qualified certificate,

b) following revocation of certificates per (a) above, confirmation of the date and time of their revocation within 30 days from revocation,

c) information on the termination of use of data used to execute the electronic signature or electronic seal of a qualified trust service corresponding to the data for validation of electronic signature or electronic seal from the certificates identified for this service in the trusted list within 30 days from termination of use of such data; this provision does not apply if the date and time of the expiry of the final certificate identified for this service in the trusted list matches the date and time for terminating the usage of data to execute electronic signature or electronic seal.

(3) Information per Sections (1) and (2) above is submitted to the Authority using the electronic form or in writing using the template published by the Authority on the central public administration portal and on its website.

§7

(1) Qualified trust service providers that issue qualified certificates, when providing information on the validity or revocation status of qualified certificates[18]), shall also provide information containing confirmation of the date and time until which the certificates were recorded as valid or information on the date and time at which the qualified certificate was revoked.

(2) Qualified trust service providers to which the Authority conferred qualified status may not temporarily suspend a qualified certificate for electronic signature or a qualified certificate for electronic seal.

§8

Mandate certificate

(1) A mandate certificate is a qualified certificate for electronic signature issued to a natural person authorised under or on the basis of the law to act for or on the behalf of another person or public authority, or a natural person conducting activities under a special regulation,[20]) or performing a function under a special regulation[21]) ("agent"). A mandate certificate contains

a) identification data for the agent under §2 (1); if the agent is employed or in a similar working relationship with a public authority or a person for which or on whose behalf the agent acts("principal"), the identification data is a passport number or identification card number,

b) identification data

1. of the agent under §2,

2. public authority or person for whom the agent performs activities under a special regulation[20]) or performs a function under a special regulation,[21]) under §2 and

c) designation of authorisation per Section 2.

(2) The agent uses the mandate certificate to demonstrate its authorisation

a) to act on behalf or in the name of the principal,

b) to perform activities under a special regulation,[20]) or

c) to perform a function under a special regulation.[21])

(3) Qualified trust service providers to which the Authority conferred qualified status issue mandate certificates to an agent who demonstrates authorisation per Section 2 in the manner stipulated for the given authorisation in the list of authorisations maintained by the Authority under §9.

(4) Revocation of a mandate certificate is requested immediately by

a) the public authority or the person for which the agent conducted an activity or function per Section 1 after the agent is terminated or completes its activity or function per Section 1,

b) the principal after the agent's authorisation to act on behalf of or in the name of the principal expires,

c) the agent after it learns that the principal is deceased, declared dead or expired,

d) the agent after its authorisation to act on behalf of or in the name of the principal expires or if the performance of the activity or function per Section 1 expires or is terminated.

(5) A mandate certificate may not contain a pseudonym.

§9

List of authorisations

(1) The list of authorisations is a public administration information system[22]) administered by the Authority.

(2) The list of authorisations contains the following for every individual authorisation

a) designation of the agent's authorisation under §8 (2),

b) a list of documents used to demonstrate authorisation and a list of documents on the basis of which such authorisation terminates.

(3) Designation of the agent's authorisation under §8 (2) is identical to the name stipulated for the given authorisation under a specific regulation;[20]) if this is impossible, it must be identical to the name defined for the specific authorisation by a valid internal regulation or a written mandate from the public authority or another person on whose behalf or in whose name the authorisation is performed.

(4) Documents per Section 2 (b) are identical to the documents on the basis of which the specific authorisation is formed and expires under a specific regulation[20]). If authorisation is based on entry in records mandated by law, the document is always the excerpt from these records issued by the public authority maintaining such records.

(5) The Authority shall record the details specified in Section 2 into the list of authorisations and update them. For the purposes of fulfilling the Authority's obligations per the first sentence, state and local government authorities are obliged to immediately inform the Authority of the existence of authorisations under §8 (2) as stipulated in generally binding legal regulations in the area in which they conduct state or local governance and any changes thereto.

(6) The Authority publishes the list of authorisations on its website.

§10

Certification

(1) The Authority certifies conformity between a device to complete qualified electronic signature[23]) or a device to complete qualified electronic seal[24]) with the requirements under a special regulation[25]) based on an application in the certification process.

(2) The Authority certifies compliance of the application to complete qualified electronic signature or qualified electronic seal with the requirements under a special regulation[26] based on an application within the certification process; a technical standard[27]) is the tool used for conformity assessment per the first sentence.

(3) The Authority verifies and evaluates compliance between the electronic registry and the requirements defined herein on the basis of the application filed within the certification process.

(4) The application for certification per Sections 1 to 3 is submitted to the Authority using the electronic form or in writing using the template published by the Authority on the central public administration portal and on its website.

(5) The applicant provides the following with the application for certification per Sections 1 to 3

a) the subject of certification if required by procedures,

b) technical documentation for the subject of certification required for certification and the security audit, if required by procedures.

(6) Proceedings under Sections 1 to 3 commence on the day a complete application is submitted. If the application is incomplete, the Authority shall call on the applicant to amend its application in a term of no less than ten days. Applications that are not amended within the defined term are disregarded.

(7) The Authority shall issue a decision in proceedings under Sections 1 to 3 within 90 days of receipt of a complete application. If the Authority determines the conformity of a device to complete a qualified electronic signature, a device to complete a qualified electronic seal, applications to complete and verify qualified electronic signature or qualified electronic seal and the conformity of the electronic registry within the proceedings, the Authority issues a certificate valid for five years.

(8) If security requirements do not change during the valid term of a certificate issued by the Authority on the basis of proceedings as defined in Sections 1 to 3, the Authority may decide on such application in an abbreviated proceeding within 60 days of receipt of a complete application to extend certificate validity by an additional five years; Subsections 5 to 7 apply mutatis mutandis.

§11
Authority

The Authority

a) is the supervisory body under a special regulation,[28])

b) issues trust service certificates for which qualified status is conferred if a trust service provider requests issuance of a certificate,

c) issues and publishes a special certificate for verification of certificates issued under (b) above in the infrastructure established under (f) below,

d) revokes certificates issued to trust service providers whose qualified status has been withdrawn,

e) certifies and assesses conformity under a special regulation[29]) and under this Act,

f) establishes, maintains and updates trust infrastructure[30]) in which a list of all qualified certificates issued by trust service providers conferred qualified status is maintained along with information on the validity or revocation status of issued qualified certificates updated after expiry or revocation of the qualified certificates at a minimum,

g) provides information from trust infrastructure, in particular information after expiry[18]) of a qualified certificate in the form of an affirmative confirmation[31]) of the validity or revocation status of qualified certificates,[32])

h) secures tasks connected with archiving documents under this Act in trust infrastructure if a qualified trust service provider expires[33]) without a legal successor,

i) creates, maintains and publishes the trusted list under a special regulation,[34])

j) provides the European Commission with information, reports and notices under a special regulation,[35])

k) issues methodology and standards under this Act and publishes them on its website,

l) issues, administers and publishes certification policies used to identify conformity of certificates issued by qualified trust service providers with the requirements under this Act,

m) issues, administers and publishes signature policies that contain in particular a list of algorithms and their minimal parameters for electronic signature from the level of the security of advanced electronic signature and for electronic seal from the level of the security of advanced electronic seals to be complied with in dealings with public authorities from the moment of their publication by the Authority.

§12

Audit and supervision

(1) When conducting audits for compliance with the provisions hereof, the Authority operates on the basis of the basic rules for audit activities stipulated in a special regulation.[36])

(2) Trust service providers have the rights and obligations of an audited party under a special regulation[37]) for the purposes of conducting the audit.

(3) The Authority conducts supervision under a special regulation.[38])

§13

Offences and Administrative Offences

(1) An offence is committed by anyone using the EU trust mark[39]) in violation of Article 23 (1) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257, 28 August 2014) ("Regulation (EU) No. 910/2014").

(2) An offence is committed by anyone who violates the conditions and restrictions on using qualified trust services under Article 24 (2)(d) of Regulation (EU) No. 910/2014.

(3) Offences under Sections 1 and 2 above may be subject to a fine of up to €2,000.

(4) The general regulation on offences[40]) is applied to offences and related hearings.

(5) The Authority hears offences as defined in Sections 1 and 2 above.

§14

(1) The Authority shall levy a fine of up to €3,000 on legal entities or individual entrepreneurs who commit an administrative offence by using the EU trust mark[39]) in violation of Article 23 (1) of Regulation (EU) No. 910/2014.

(2) The Authority shall levy a fine of up to €3,000 on legal entities or individual entrepreneurs who commit an administrative offence by violating the conditions and restrictions on using qualified trust services under Article 24 (2)(d) of Regulation (EU) No. 910/2014.

(3) The Authority shall levy a fine of up to €3,000 on public authorities that commit an administrative offence by refusing to accept a qualified electronic signature or qualified electronic seal in a format that complies with the implementing acts issued by the Commission under Article 27 (5) and Article 37 (5) of Regulation (EU) No. 910/2014.

(4) The Authority shall levy a fine of up to €3,000 on public authorities that commit an administrative offence by creating a qualified electronic signature or qualified electronic seal in a format that does not comply with the implementing acts issued by the Commission under Article 27 (5) and Article 37 (5) of Regulation (EU) No. 910/2014.

(5) The Authority shall levy a fine of up to €33,000 on trust service providers that commit an administrative offence by

a) not taking appropriate technical and organisational measures to mitigate the risks posed to the security of the trust services they provide under Article 19 (1) of Regulation (EU) No. 910/2014,

b) not reporting security incidents to the supervisory body or other stakeholder in violation of Article 19 (1) of Regulation (EU) No. 910/2014,

c) providing qualified trust services before qualified status is published in the trusted list in violation of Article 21 (1) of Regulation (EU) No. 910/2014.

(6) The Authority shall levy a fine of up to €66,000 on qualified trust service providers that commit an administrative offence by

a) violating the obligations contained in §5, §6 (1) or (2) or §7,

b) in violation of Article 20 (1) of Regulation (EU) No. 910/2014

1. not submitting to an audit by the authority assessing conformity at least once every 24 months or

2. failing to file the resulting conformity assessment report to the supervisory body within three business days from its receipt,

c) not submitting to an audit by the supervisory body or conformity assessment body under Article 20 (2) of Regulation (EU) No. 910/2014,

d) not ensuring that a link to the relevant trusted list is made available on its website under Article 23 (2) of Regulation (EU) No. 910/2014,

e) not verifying the identify of a natural person or the identification details of a legal entity when issuing a qualified certificate under Article 24 (1) of Regulation (EU) No. 910/2014,

f) failing to inform the supervisory body of all changes in providing its qualified trust services and the intention to terminate such activities under Article 24 (2)(a) of Regulation (EU) No. 910/2014, g) employing personnel and having subcontractors in violation of Article 24 (2)(b) of Regulation (EU) No. 910/2014,

h) in violation of Article 24 (2)(c) of Regulation (EU) No. 910/2014

1. failing to maintain sufficient funding or

2. failing to conclude suitable liability insurance cover for damages,

i) failing to fulfil the obligation to inform under Article 24 (2) (d) of Regulation (EU) No. 910/2014,

j) failing to use trustworthy systems and products under Article 24 (2)(e) of Regulation (EU) No. 910/2014,

k) failing to use trustworthy systems to archive data under Article 24 (2)(f) of Regulation (EU) No. 910/2014,

l) failing to take appropriate measures against forgery and theft of data under Article 24 (2)(g) of Regulation (EU) No. 910/2014,

m) failing to record, archive and keep accessible all relevant information under Article 24 (2)(h) of Regulation (EU) No. 910/2014,

n) not having an up-to-date termination plan to ensure continuity of service under Article 24 (2)(i) of Regulation (EU) No. 910/2014,

o) not establishing or updating the database of certificates in violation of Article 24 (2)(k) of Regulation (EU) No. 910/2014,

p) failing to publish revocation of an issued qualified certified under Article 24 (3) of Regulation (EU) No. 910/2014,

q) failing to provide the relying party with information on the validity or revocation status of qualified certificates it issued under Article 24 (4) of Regulation (EU) No. 910/2014,

r) reverting revocation status of a qualified certificate for electronic signature in violation of Article 28 (4) of Regulation (EU) No. 910/2014,

s) failing to provide validation of a qualified electronic signature or qualified electronic seal under Article 33 (1)(a) of Regulation (EU) No. 910/2014,

t) preventing the relying parties from receiving the result of the validation process under Article 33 (1)(b) of Regulation (EU) No. 910/2014,

u) failing to use the procedures and technologies required under Article 34 (1) of Regulation (EU) No. 910/2014,

v) reverting revocation status of a qualified certificate for electronic seal in violation of Article 38 (4) of Regulation (EU) No. 910/2014,

w) failing to ensure qualified electronic time stamp[41]) it issued meets the requirements of Article 42

1. of Regulation (EU) No. 910/2014, or

x) failing to ensure qualified certificates it issued contained accurate, truthful and complete information.

(7) The Authority considers the severity, manner, duration and consequences of a violation when levying a fine for an administrative offence.

(8) The Authority shall levy a fine of up to double the amount laid out in Sections (1) to (6) if a repeat violation of obligations for which a fine was previously levied under Sections (1) to (6) reoccurs within a period of one year from the date of the decision imposing the fine.

(9) Fines for administrative offences may be levied within two years from the date on which a violation is discovered and no later than four years from the date on which the violation occurred.

(10) Payment terms for a fine for an administrative offence is 30 days from the date of the decision imposing the fine.

(11) Fines for administrative offences constitute state budget revenue.

§15
Electronic registry

The electronic registry is used to secure activities related to receiving, sending and confirming receipt of electronic documents and electronic documents signed with a qualified electronic signature or sealed with a qualified electronic seal.

§16
Authorisation Provisions

The Authority is authorised to issue a generally binding legal regulation,

a) laying down the details of verification of qualified electronic signature or qualified electronic seal, the formats of qualified electronic signature or qualified electronic seal, the formats of qualified certificates, the formats of information on validity or revocation status of qualified certificates,[18]) trusted list extensions, procedures for archiving electronic signatures, seals or certificates and the formats of signature policies for national expansion for trust infrastructure and trust services,

b) laying down the details of securing electronic registry activities related to receiving, sending and confirming receipt of electronic documents and electronic documents signed with a qualified electronic signature or sealed with a qualified electronic seal.

§17
Common Provisions

(1) Proceedings as defined herein are subject to the general regulation on administrative procedure,[42]) unless otherwise defined herein.

(2) If generally binding legal regulations use the following terms

a) advanced electronic signature, such reference is understood as qualified electronic signature,

b) advanced electronic seal, such reference is understood as qualified electronic seal,

c) time stamp, such reference is understood as qualified electronic time stamp.

§18
Transitional provisions

(1) A provider of accredited certification services under existing regulations in the scope of existing accreditation under existing regulations is considered a certified trust service provider to which the Authority conferred qualified status providing qualified trust services. A provider as defined in the first sentence is obliged to file a conformity assessment report[43]) to the Authority by 1 July 2017 at the latest;[44]) if such report is not provided, its standing as a trust service provider conferred qualified status and providing qualified trust services expires on 2 July 2017.

(2) An accredited service for issuing time stamps accredited by the Authority and maintained in the list of trusted information on certification service providers under a special regulation[45]) is considered a trust service for issuing qualified electronic time stamps[41]) conferred qualified status. A service provider as defined in the first sentence is obliged to file a conformity assessment report[43]) to the Authority by 1 July 2017 at the latest;[44]) if such report is not provided, its standing as a trust service provider conferred qualified status in relation to this service expires on 2 July 2017.

(3) Secure devices to complete electronic stamps under existing regulations are considered devices to complete a qualified electronic stamp under a special regulation[27]) until expiry of the validity or revocation of the certificate for the device.

(4) A qualified system certificate issued under existing regulations is considered a qualified certificate for a qualified electronic stamp under a special regulation[11]) until expiry of its validity or its revocation.

(5) Information on validity or revocation status of a qualified certificate[18]) in the Online Certificate Status Protocol (OCSP) reply[32]) must contain an affirmative statement as to the existence and accuracy of the data[31]) that must be provided beginning on 1 January 2018.

§18a

Transitional provisions for adjustments effective since 1 August 2019

In connection with conducting of activities under § 11 (2) as in force until 31 July 2019, the Authority shall transfer the related operational documentation, including the personal data used, to the acquirer by written agreement.

§19

Repealing Provisions

The following are repealed:

1. Act No.215/2002 Coll. on Electronic Signature and on amendment of certain acts as amended by Act No.679/2004 Coll., Act No.25/2006 Coll., Act No.275/2006 Coll., Act No.214/2008 Coll., Act No.289/2012 Coll., Act No.305/2013 Coll., Act No.273/2015 Coll. and Act No.91/2016 Coll.,

2. National Security Authority Decree No. 131/2009 Coll. on the Format, Contents and Management of Certificates and Qualified Certificates and Format, Periodicity and Manner of Publication of the List of Cancelled Qualified Certificates (concerning certificates and qualified certificates) as amended by Decree No. 323/2012 Coll. and Decree No. 60/2014 Coll.,

3. National Security Authority Decree No. 132/2009 Coll. on Conditions for Providing Accredited Certification Services and on Audit Requirements, the Scope of Audit and Auditor Qualification as amended by Decree No. 61/2014 Coll.,

4. National Security Authority Decree No. 133/2009 Coll. on the Contents and Scope of Operating Documentation Maintained by the Certification Authority and on Security Rules and Rules for Conducting Certification Activities as amended by Decree No. 62/2014 Coll.,

5. National Security Authority Decree No. 134/2009 Coll. defining the details of requirements for secure devices to complete time stamps and the requirements on products for electronic signature (on electronic signature products) as amended by Decree No. 63/2014 Coll.,

6. National Security Authority Decree No. 135/2009 Coll. on the Format and Manner of Completing Advanced Electronic Signature, the Manner of Publication of the Authority's Public Key, Validity Conditions for Advanced Electronic Signature, the Procedure for Verification and Conditions for Verifying Advanced Electronic Signature, the Time Stamp Format and Manner of its Completion, Requirements on Time Stamp Sources and Requirements for Maintaining Time Stamp Documentation (on completion and verification of electronic signature and time stamp) as amended by Decree No. 32/2010 Coll. and Decree No. 64/2014 Coll.,

7. National Security Authority Decree No. 136/2009 Coll. on the Manner and Procedure for Use of Electronic Signature in Business Dealings and Administrative Dealings as amended by Decree No. 248/2015 Coll.

Article II

National Council of the Slovak Republic Act No.145/1995 Coll. on Administrative Fees as amended by National Council of the Slovak Republic Act No.123/1996 Coll., National Council of the Slovak Republic Act No.224/1996 Coll., Act No.70/1997 Coll., Act No.1/1998 Coll., Act No.232/1999 Coll., Act No.3/2000 Coll., Act No.142/2000 Coll., Act No.211/2000 Coll., Act No.468/2000 Coll., Act No.553/2001 Coll., Act No.96/2002 Coll., Act No.118/2002 Coll., Act No.215/2002 Coll., Act No.237/2002 Coll., Act No.418/2002 Coll., Act No.457/2002 Coll., Act No.465/2002 Coll., Act No.477/2002 Coll., Act No.480/2002 Coll., Act No.190/2003 Coll., Act No.217/2003 Coll., Act No.245/2003 Coll., Act No.450/2003 Coll., Act No.469/2003 Coll., Act No.583/2003 Coll., Act No.5/2004 Coll., Act No.199/2004 Coll., Act No.204/2004 Coll., Act No.347/2004 Coll., Act No.382/2004 Coll., Act No.434/2004 Coll., Act No.533/2004 Coll., Act No.541/2004 Coll., Act No.572/2004 Coll., Act No.578/2004 Coll., Act No.581/2004 Coll., Act No.633/2004 Coll., Act No.653/2004 Coll., Act No.656/2004 Coll., Act No.725/2004 Coll., Act No.5/2005 Coll.,

Act No.8/2005 Coll., Act No.15/2005 Coll., Act No.93/2005 Coll., Act No.171/2005 Coll., Act No.308/2005 Coll., Act No.331/2005 Coll., Act No.341/2005 Coll., Act No.342/2005 Coll., Act No.468/2005 Coll., Act No.473/2005 Coll., Act No.491/2005 Coll., Act No.538/2005 Coll., Act No.558/2005 Coll., Act No.572/2005 Coll., Act No.573/2005 Coll., Act No.610/2005 Coll., Act No.14/2006 Coll., Act No.15/2006 Coll., Act No.24/2006 Coll., Act No.117/2006 Coll., Act No.124/2006 Coll., Act No.126/2006 Coll., Act No.224/2006 Coll., Act No.342/2006 Coll., Act No.672/2006 Coll., Act No.693/2006 Coll., Act No.21/2007 Coll., Act No.43/2007 Coll., Act No.95/2007 Coll., Act No.193/2007 Coll., Act No.220/2007 Coll., Act No.279/2007 Coll., Act No.295/2007 Coll., Act No.309/2007 Coll., Act No.342/2007 Coll., Act No.343/2007 Coll., Act No.344/2007 Coll., Act No.355/2007 Coll., Act No.358/2007 Coll., Act No.359/2007 Coll., Act No.460/2007 Coll., Act No.517/2007 Coll., Act No.537/2007 Coll., Act No.548/2007 Coll., Act No.571/2007 Coll., Act No.577/2007 Coll., Act No.647/2007 Coll., Act No.661/2007 Coll., Act No.92/2008 Coll., Act No.112/2008 Coll., Act No.167/2008 Coll., Act No.214/2008 Coll., Act No.264/2008 Coll., Act No.405/2008 Coll., Act No.408/2008 Coll., Act No.451/2008 Coll., Act No.465/2008 Coll., Act No.495/2008 Coll., Act No.514/2008 Coll., Act No.8/2009 Coll., Act No.45/2009 Coll., Act No.188/2009 Coll., Act No.191/2009 Coll., Act No.274/2009 Coll., Act No.292/2009 Coll., Act No.304/2009 Coll., Act No.305/2009 Coll., Act No.307/2009 Coll., Act No.465/2009 Coll., Act No.478/2009 Coll., Act No.513/2009 Coll., Act No.568/2009 Coll., Act No.570/2009 Coll., Act No.594/2009 Coll., Act No.67/2010 Coll., Act No.92/2010 Coll., Act No.136/2010 Coll., Act No.144/2010 Coll., Act No.514/2010 Coll., Act No.556/2010 Coll., Act No.39/2011 Coll., Act No.119/2011 Coll., Act No.200/2011 Coll., Act No.223/2011 Coll., Act No.254/2011 Coll., Act No.256/2011 Coll., Act No.258/2011 Coll., Act No.324/2011 Coll., Act No.342/2011 Coll., Act No.363/2011 Coll., Act No.381/2011 Coll., Act No.392/2011 Coll., Act No.404/2011 Coll., Act No.405/2011 Coll., Act No.409/2011 Coll., Act No.519/2011 Coll., Act No.547/2011 Coll., Act No.49/2012 Coll., Act No.96/2012 Coll., Act No.251/2012 Coll., Act No.286/2012 Coll., Act No.336/2012 Coll., Act No.339/2012 Coll., Act No.351/2012 Coll., Act No.439/2012 Coll., Act No.447/2012 Coll., Act No.459/2012 Coll., Act No.8/2013 Coll., Act No.39/2013 Coll., Act No.40/2013 Coll., Act No.72/2013 Coll., Act No.75/2013 Coll., Act No.94/2013 Coll., Act No.96/2013 Coll., Act No.122/2013 Coll., Act No.144/2013 Coll., Act No.154/2013 Coll., Act No.213/2013 Coll., Act No.311/2013 Coll., Act No.319/2013 Coll., Act No.347/2013 Coll., Act No.387/2013 Coll., Act No.388/2013 Coll., Act No.474/2013 Coll., Act No.506/2013 Coll., Act No.35/2014 Coll., Act No.58/2014 Coll., Act No.84/2014 Coll., Act No.152/2014 Coll., Act No.162/2014 Coll., Act No.182/2014 Coll., Act No.204/2014 Coll., Act No.262/2014 Coll., Act No.293/2014 Coll., Act No.335/2014 Coll., Act No.399/2014 Coll., Act No.40/2015 Coll. Act No.79/2015 Coll., Act No.120/2015 Coll., Act No.128/2015 Coll., Act No.129/2015 Coll., Act No.247/2015 Coll., Act No.253/2015 Coll., Act No.259/2015 Coll., Act No.262/2015 Coll., Act No.273/2015 Coll., Act No.387/2015 Coll., Act No.403/2015 Coll. and Act No.125/2016 Coll. is amended as follows:

1. In the Overview of Administrative Fee Charges in Section XX the words “Electronic signature” are replaced by the words “Trust services”.

2. In the Overview of Administrative Fee Charges. Section XX. including the title reads:

“SECTION XX TRUST SERVICES

Line item 268

a Award of qualified status
b Certification €665 €332".

Article III

Act No.575/2001 Coll. on the Organisation of the Activities of Government and Central State Authorities as amended by Act No.143/2002 Coll., Act No.411/2002 Coll., Act No.465/2002 Coll., Act No.139/2003 Coll., Act No.453/2003 Coll., Act No.523/2003 Coll., Act No.215/2004 Coll., Act No.351/2004 Coll., Act No.405/2004 Coll., Act No.585/2004 Coll., Act No.654/2004 Coll., Act No.78/2005 Coll., Act No.172/2005 Coll., Act No.474/2005 Coll., Act No.231/2006 Coll., Act No.678/2006 Coll., Act No.103/2007 Coll., Act No.218/2007 Coll., Act No.456/2007 Coll., Act No.568/2007 Coll., Act No.617/2007 Coll., Act No.165/2008 Coll., Act No.408/2008 Coll., Act No.583/2008 Coll., Act No.70/2009 Coll., Act No.165/2009 Coll., Act No.400/2009 Coll.,

Act No.403/2009 Coll., Act No.505/2009 Coll., Act No.557/2009 Coll., Act No.570/2009 Coll., Act No.37/2010 Coll., Act No.372/2010 Coll., Act No.403/2010 Coll., Act No.547/2010 Coll., Act No.392/2011 Coll., Act No.287/2012 Coll., Act No.60/2013 Coll., Act No.311/2013 Coll., Act No.313/2013 Coll., Act No.335/2014 Coll., Act No.172/2015 Coll., Act No.339/2015 Coll., Act No.358/2015 Coll., Act No.392/2015 Coll. and Act No.171/2016 Coll. is amended as follows:

In §34, the words "electronic signature" are replaced with the words "trust services".

Article IV

Act 224/2006 Coll. on Identification Cards and on amendment of certain acts as amended by Act No.693/2006 Coll., Act No.647/2007 Coll., Act No.445/2008 Coll., Act No.49/2012 Coll., Act No.336/2012 Coll. and Act No.125/2015 Coll. is amended as follows:

1. §4b (2) reads:

2. "(2) A personal security code is a combination of at least six and at most ten digits. A citizen who at the time of applying for the issuance of an identification card has not attained 65 years of age may select a personal security code when filing the application; other citizens may select a personal security code when filing the application or later at the district directorate. The personal security code for a citizen deprived of legal capacity is selected by their guardian.".

3. In §6 (1), the words "district directorate in the area where the citizen has their permanent address" are replaced by the words "any district directorate".

4. Section 6 is deleted from §17a.

5. §17b is inserted after §17a with the following text:

"§17b

Transitional Provisions for Regulations Effective on the Date of Declaration

(1) The district directorate shall issue an identification under the provisions hereof effective at the date of the application to issue an identification card to the citizen requesting an identification card under existing regulations.

(2) A citizen who has been issued an identification card with an electronic chip under existing regulations and who has not selected a personal security code may select a personal security code at a district directorate.

(3) The procedure laid down in §4b (2) shall be applied when submitting applications to issue an identification card via the Ministry's portal (§7b) beginning on 1 July 2017 at the latest.".

Article V

Act No.305/2013 Coll. on the Electronic Form of Governance Conducted by Public Authorities and on amendment of certain acts (e-Government Act) as amended by Act No.214/2014 Coll., Act No.29/2015 Coll., Act No.130/2015 Coll. and Act No.273/2015 Coll. is amended as follows:

1. §22aa is inserted after §22a with the following text:

"§22aa

Authentication Certificate

(1) An authentication certificate is an electronic document proving the electronic identity of the party to which it was issued and is used for identification and authentication purposes when accessing an information system or in electronic communication related to the exercise of official authority or for the purposes of accessing an electronic mailbox or disposition of an electronic mailbox.

(2) The authentication certificate contains information that an authentication certificate is involved and an identifier for the person to whom it was issued.".

2. In §13 (4), §19 (4)(b), §22a (1) and (2), §22b (2) to (6) and §60a (7) and (8), reference 12b including the footnote to reference 12b is deleted.

3. In §31 (3), the words " executing its advanced conversion (§35 (2)) under this Act and delivers the output from this conversion in paper form; delivery of the output from advanced conversion" are replaced by the words "completion of a copy of the electronic document in paper form and delivers this copy; delivery of a copy".

4. In §35 (3)(a), a dash is inserted and the word "lawyer" is added after the words "public authority" while the words "lawyer or" are deleted from §35 (3)(c).

5. In §37 (1)(h) the semi-colon is deleted and the words "if advanced conversion was completed in an automated manner, this data does not appear".

6. In §59, Section 3 is amended to add letter h), which reads:

"h) details of the method for issuing authentication certificates under §22aa.".

7. In §60 (12), the words "three years from the effective date of this Act" are replaced by the words "by 31 January 2018" and the words "three years from the effective date of this Act" are replaced by the words "the period laid down in the first sentence".

8. In §60a (5), the words "Section 1" are replaced by the words "Section 4".

9. §60b to §60d are added after §60a, including the title above §60b, which reads:

"Transitional provisions for regulations effective on the date of declaration

§60b

(1) A public authority operating a specialised portal is not obliged to connect the public administration information portal[3]) it administers to the central portal by 31 January 2018 if electronic communication with the central portal is facilitated in a different way.

(2) A public authority is authorised from 1 November 2016 to 31 January 2018 to proceed in the electronic exercise of official authority under special regulations if they lay down different procedures for public authorities during the electronic exercise of official authority and different details in the electronic versions of petitions to start proceedings, claims, applications, complaints, responses, statements, reports or other similar documents, submitted to the public authority within such proceedings or different details in the electronic versions of decisions, applications, responses, statements or other documents that are issued by the public authority within such proceedings or this Act.

(3) If legal entities that do not have activated electronic mailboxes are involved and that are not registered in the Commercial Register, the administrator of the electronic mailbox module will activate their electronic mailboxes on 1 May 2018; this applies for legal entities that are not registered in the Commercial Register; fulfilment of the conditions for activation of electronic mailboxes will occur after the effective date hereof and by 30 April 2018. The provisions of §60a (5) do not apply to legal entities identified in the first sentence. If a legal entity as defined in the first sentence requests early activation of its electronic mailbox, the administrator of the electronic mailbox shall comply with its request and the provisions of §13 (3) apply mutatis mutandis. Information as to which legal entities are subject to the approach identified in the first to third sentences shall be published and updated by the electronic mailbox module administrator on the central portal.

§60c

(1) The National Security Authority ("Authority") maintains a register of certificates. The register of certificates is a public administration information system[3]) administered by the Authority. The Authority maintains a list of qualified certificates for electronic seal[33]) issued by public authorities in the register of certificates.

(2) A public authority is authorised to enter qualified certificates for electronic seal[33]) that were issued to it in the register of certificates and is obliged to notify the Authority without any undue delay of any revocation of the recorded certificates. The Authority enters qualified certificates for electronic seal[33]) into the register upon request from the pubic authority to which they were issued and immediately deletes the record from the register after notification of the revocation of the recorded certificate is received.

(3) Verification of a qualified electronic seal with a qualification certificate for the electronic seal 33) recorded in the register of certificates is performed using the list of valid qualification certificates for electronic seal.

(4) The Authority is obliged to publish a list of qualified certificates for electronic seal recorded in the register of certificates on a daily basis and publish it on its website.

(5) The list of valid qualified certificates for electronic seal is valid for 24 hours from its publications and a qualified certificate for electronic seal[33]) contained in this list is considered valid for the duration of the validity of the list, unless proven otherwise.

§60d

Transitional provisions for regulations effective as of 1 March 2017

The Office of the Deputy Prime Minister of the Slovak Republic for Investment and Informatisation ("Office of the Deputy Prime Minister") shall establish a central register of records of completed advanced conversions and begin assigning record numbers of records of completed advanced conversions under §39 (6) by 1 January 2018 at the latest; the Office of the Deputy Prime Minister shall report the establishment of the register and the assignment of record numbers on its website and on the central portal. Until the day after the date on which the central register of records of completed advanced conversions is established, a party conducting conversion is not obliged to proceed in accordance with §36 (5) and the Chamber of Notaries of the Slovak Republic is not obliged to proceed in accordance with §39 (6).".

Footnote 33 reads:

"[33]) Article 3 (30) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257, 28 August 2014).".

10. The words "list of reference registers" in all forms in the entire text of the Act are replaced by the words "list of reference data" in the appropriate form.

11. The words "authenticated qualified certificate" in all forms in the entire text of the Act are replaced by the words "authenticated certificate under §22aa" in the appropriate form and the words "register of authenticated qualified certificates" in all forms in the entire text of the Act are replaced by the words "register of authenticated certificates" in the appropriate form.

Article VI

(1) This Act shall take effect on the date of declaration, except for §60d in Article V (9), which takes effect on 1 March 2017.

(2) The provisions laid down in §60c in Article V (9) expire on 31 December 2017.

Andrej Kiska

Andrej Danko

Robert Fico

1) Article 3 (16) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ EU L 257, 28 August 2014).
2) Article 3 (19) of Regulation (EU) No. 910/2014.
3) Regulation (EU) No. 910/2014.
4) Article 3 (12) of Regulation (EU) No. 910/2014.
5) Article 3 (15) of Regulation (EU) No. 910/2014. Annex to Regulation (EU) No. 910/2014.
6) Article 3 (20) of Regulation (EU) No. 910/2014.
7) Article 21 (2) second subsection of Regulation (EU) No. 910/2014.
8) Article 28 (3) of Regulation (EU) No. 910/2014.
9) Article 3 (9) of Regulation (EU) No. 910/2014.
10) Article 3 (27) of Regulation (EU) No. 910/2014.
11) Article 3 (30) of Regulation (EU) No. 910/2014.
12) Article 38 (3) of Regulation (EU) No. 910/2014.
13) Article 3 (24) of Regulation (EU) No. 910/2014.
14) Article 21 (1) of Regulation (EU) No. 910/2014.
15) Article 3 (17) of Regulation (EU) No. 910/2014.
16) Article 22 of Regulation (EU) No. 910/2014.
17) Recommendation ITU-TX.509 | ISO/IEC 9594-8: Information technology - Open systems integration - The directory: Public-key and attribute certificate frameworks.
18) Article 24 (4) of Regulation (EU) No. 910/2014.
19) Article 24 (2)(h) of Regulation (EU) No. 910/2014.
20) For instance, Slovak National Council Act No. 323/1992 Coll. on Notaries and Notary Activities (Notary Code) as amended, National Council of the Slovak Republic Act No. 233/1995 Coll. on Court-Appointed Executors and Execution Activities (Execution Code) and on amendment of certain acts as amended, Act No. 586/2003 Coll. on Advocacy and on amendment of Act No. 455/1991 Coll. on Trade Licensing (Trade License Act) as amended, as amended, Act No. 382/2004 Coll. on Experts, Interpreters and Translators and on amendment of certain acts as amended.
21) For instance Act No. 385/2000 Coll. on Judges and Lay Judges and on amendment of certain acts as amended, Act No. 153/2001 Coll. on Prosecution as amended.
22) §2 (1)(b) of Act No. 275/2006 Coll. on Public Administration Information Systems and on amendment of certain acts as amended.
23) Article 3 (23) of Regulation (EU) No. 910/2014.
24) Article 3 (32) of Regulation (EU) No. 910/2014.
25) Article 29, 30 and 39 of Regulation (EU) No. 910/2014.
26) Article 32 of Regulation (EU) No. 910/2014.
27) Annex A to ISO 14533 (Processes, data elements and documents in business, industry and administration - long-term signature profiles) and official standards, in particular QES/QESe verification, QES/QESe formats, Qualified certificate formats, CRL/OCSP formats, Expansion of the trusted list and Signature policy formats.
28) Article 17 of Regulation (EU) No. 910/2014.
29) Article 30 and 39 of Regulation (EU) No. 910/2014.
30) Article 17 (5) of Regulation (EU) No. 910/2014.
31) CertHash (positive statement), Chapter 3.1.2, Common PKI Specification V2.0.
32) RFC 6960 X.509 Internet PublicKeyInfrastructure, OnlineCertificate Status Protocol - OCSP.
33) Article 24 (2)(i) of Regulation (EU) No. 910/2014.
34) Article 22 of Regulation (EU) No. 910/2014. Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ EU L 235, 9 September 2015).
35) Article 17 (2) and (4)(d), Article 19 (3), Article 22 (3), Article 30 (2) and Article 31 (1) of Regulation (EU) No. 910/2014.
36) §8 to 13 of National Council of the Slovak Republic Act No. 10/1996 Coll. on Government Audits as amended.
37) §12 of Act No. 10/1996 Coll.
38) Article 17, Article 19 and Article 20 of Regulation (EU) No. 910/2014.
39) Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services (OJ EU, L 128, 23 May 2015).
40) Slovak National Council Act No. 372/1990 Coll. on Offences as amended.
41) Article 3 (34) of Regulation (EU) No. 910/2014.
42) Act No. 71/1967 Coll. on Administrative Procedure (Code of Administrative Procedure) as amended.
43) Article 20 (1) of Regulation (EU) No. 910/2016.

44) Article 51 (3) of Regulation (EU) No. 910/2016.

45) Commission Implementing Decision 2013/662/EU of 14 October 2013 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States (OJ EU L 306, 16 November 2013).

The published of the Collection of Laws of the Slovak Republic, content administrator and operator of the Slov-Lex legal and information portal accessible at www.slov-lex.sk is the Ministry of Justice of the Slovak Republic, Župné námestie 13, 813 11 Bratislava, tel.: 02 888 91 137, fax: 02/52442853, e-mail: helpdesk@slov-lex.sk.