Verzia 2.0

Požiadavky na prevádzku poskytovateľov dôveryhodných služieb definované orgánom dohľadu

28.2.2017

Sekcia kybernetickej bezpečnosti
Budatínska č. 30 | 851 06 Bratislava | Slovenská republika
tel.: +421 2 6869 1111 | fax: +421 2 6869 1700
e-mail: podatelna@nbu.gov.sk | http://www.nbu.gov.sk/

Obsah

1 Úvod

Požiadavky na prevádzku poskytovateľov kvalifikovaných a nekvalifikovaných dôveryhodných služieb definované orgánom dohľadu (ďalej len „požiadavky na prevádzku“) mapujú základné požiadavky v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.
Ide najmä o materiálno-technické zabezpečenie vhodných objektov, primerané finančné prostriedky, poistenie zodpovednosti, zodpovedajúcu odbornosť personálu a ostatné požiadavky pre kvalifikovaných a nekvalifikovaných poskytovateľov dôveryhodných služieb.

Upozornenie: Text požiadaviek bude priebežne dopĺňaný.

2 Predmet dokumentu

Požiadavky na prevádzku ako samostatný dokument dopĺňajú Schému dohľadu kvalifikovaných dôveryhodných služieb, ktorá definuje pravidlá uplatňované orgánom dohľadu pri dohľade kvalifikovaných dôveryhodných služieb a je základom pre Certifikačnú schému orgánu posudzovania zhody.

3 Odkazy

Požiadavky na prevádzku zodpovedajú požiadavkám podľa:

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „eIDAS“ alebo „nariadenie eIDAS“).

[2] Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách, ďalej len „ZDS“).

[3] Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z. (ďalej len „zákon č. 122/2013 Z. z.“).

[4] Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Text s významom pre EHP).

[5] Vykonávacie nariadenie komisie (EÚ) 2015/806 z 22. mája 2015, ktorým sa ustanovujú špecifikácie týkajúce sa formy značky dôvery EÚ pre kvalifikované dôveryhodné služby (ďalej len „Vykonávacie nariadenie komisie 2015/806“).

[6] Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane jednotlivcov vzhľadom na spracovávanie osobných údajov a o voľnom pohybe takých údajov (ďalej len „smernica 95/46/ES“).

[7] ISO/IEC 17065:2012 Conformity Assessment – Requirements for Bodies certifying Products, Processes and Services. Posudzovanie zhody – Požiadavky na orgány certifikujúce produkty, procesy a služby.

[8] ISO/IEC 27001:2013 Information Technology – Security techniques – Information Security management Systems – Requirements. Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky.

[9] ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls. Informačné technológie – Bezpečnostné metódy – Pravidlá dobrej praxe riadenia informačnej bezpečnosti.

[10] ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.

[11] ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy and Requirements for Trust Service Providers. Elektronické podpisy a infraštruktúry; Všeobecná politika a požiadavky pre poskytovateľov dôveryhodných služieb.

[12] ETSI EN 319 411-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; *Part 1: General Requirements.* Elektronické podpisy a infraštruktúry; Politika a bezpečnostné požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty. *Časť 1: Všeobecné požiadavky.*

[13] ETSI EN 319 411-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; *Part 2: Requirements for Trust Service Providers issuing EU qualified Certificates.* Elektronické podpisy a infraštruktúry; Politika a bezpečnostné požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich certifikáty. *Časť 2: Požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich kvalifikované certifikáty EÚ.*

[14] ETSI EN 319 403 V2.2.2 (2015-08) Electronic Signatures and Infrastructures (ESI); Trust Service Providers Conformity Assessment - *Requirements for Conformity Assessment Bodies assessing Trust Service Providers.* Elektronické podpisy a infraštruktúry; Posudzovanie zhody poskytovateľov dôveryhodných služieb - *Požiadavky na orgány posudzovania zhody posudzujúce poskytovateľov dôveryhodných služieb.*

[15] ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Elektronické podpisy a infraštruktúry; Politika a bezpečnostné požiadavky pre poskytovateľov dôveryhodných služieb vydávajúcich časové pečiatky.

[16] ENISA – Final draft 0.7 – 09.2016 Guidelines on initiation of qualified trust services - Guidance for Supervisory Bodies and for TSPs. Návod na začatie poskytovania kvalifikovaných dôveryhodných služieb - Príručka pre orgány dohľadu a pre poskytovateľov kvalifikovaných dôveryhodných služieb.

[17] ENISA – Final draft 0.4 – 09.2016 Guidelines on supervision of qualified trust service providers - Guidance for supervisory bodies and for TSPs. Návod k dohľadu nad poskytovateľmi

kvalifikovaných dôveryhodných služieb – Príručka pre orgány dohľadu a pre poskytovateľov kvalifikovaných dôveryhodných služieb.

[18] ENISA – Draft 0.4 – 11.2016 Guidelines for TSPs based on standards. Návod pre poskytovateľov kvalifikovaných dôveryhodných služieb založených na štandardoch.

[19] ENISA – Draft 0.1 – 11.2016 Security framework for TSPs - Guidelines on maintaining appropriate security level. Bezpečnostný rámec pre poskytovateľov kvalifikovaných dôveryhodných služieb – Návod na udržanie primeranej úrovne bezpečnosti.

[20] ENISA – Draft 0.1 – 11.2016 Auditing framework for TSPs - Guidelines on conformity assessment of TSPs. Auditný rámec pre PDS – Návod na posudzovanie zhody poskytovateľov kvalifikovaných dôveryhodných služieb.

[21] Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu - NBÚ (pozri http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf).

[22] Certifikačná schéma orgánu posudzovania zhody vytvorenú orgánom dohľadu - NBÚ (pozri http://ep.nbusr.sk/kca/tsl/CertifikacnaSchemaNBU.pdf).

4 Skratky

CAB	Conformity Assessment Body (orgán posudzovania zhody)
CP	Certificate Policy (certifikačná politika)
CRL	Certificate Revocation List (zoznam zrušených certifikátov)
CS	Certifikačná schéma orgánu posudzovania zhody vytvorená orgánom dohľadu
eIDAS	Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES
ENISA	European Union Agency for Network and Information Security (agentúra EÚ pre sieťovú a informačnú bezpečnosť) https://www.enisa.europa.eu/topics/trust-services
ISO	International Organization for Standardization (medzinárodná organizácia pre normalizáciu)
NBÚ	Národný bezpečnostný úrad
OCSP	Online Certificate Status Protocol (protokol oznamovania stavu certifikátu online)
SD	Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu
SNAS	Slovenská národná akreditačná služba
TSA	Time-Stamping Authorities (autorita časovej pečiatky)
TSP	Trust Service Provider (poskytovateľ dôveryhodných služieb)

UTC	Coordinated Universal Time (koordinovaný svetový čas)
QC	Qualified Certificate (kvalifikovaný certifikát)
QES	Qualified Electronic Signature or Qualified Electronic Seal (kvalifikovaný elektronický podpis alebo kvalifikovaná elektronická pečať)
QTS	Qualified Trust Service (kvalifikovaná dôveryhodná služba)
QTSP	Qualified Trust Service Provider (kvalifikovaný poskytovateľ dôveryhodných služieb)
ZDS	Zákon o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)

5 Mapovanie požiadaviek

Požiadavky podľa eIDAS a ZDS

Orgán dohľadu, ktorým je v Slovenskej republike NBÚ, môže stanoviť požiadavky záväzné pre QTSP na získanie kvalifikovaného štatútu. Orgán dohľadu plnenie požiadaviek overuje na základe predložených výstupov z auditu akreditovaného orgánu posudzovania zhody alebo vlastným auditom v zmysle § 12 ZDS. Orgán dohľadu stanovuje formu plnenia požiadavky nariadenia eIDAS a ZDS buď konkrétnym ustanovením spôsobu plnenia v nasledujúcich tabuľkách alebo odkazom na referenčný dokument alebo jeho časť, ktorý sa týmto stáva súčasťou certifikačnej schémy posudzovania plnenia požiadaviek na QTSP záväzných pre získanie kvalifikovaného štatútu. Možný spôsob plnenia požiadaviek sa v tabuľkách uvádza v zátvorkách "{}", ak je ho potrebné odlíšiť od povinných požiadaviek.

5.1 Požiadavky orgánu dohľadu (NBÚ) na kvalifikovaných poskytovateľov dôveryhodných služieb

Tabuľka T1

Identifikátor požiadavky	Požiadavka orgánu dohľadu (NBÚ) na kvalifikovaných poskytovateľov dôveryhodných služieb { možná realizácia požiadavky nariadenia }
Čl. 21 eIDAS, § 3 ods. 1 ZDS	*Oznámenie o zámere poskytovať vybrané kvalifikované dôveryhodné služby:* – formulár v listinnej alebo elektronickej forme (vzor je v Prílohe A), * – konkrétne vybrané kvalifikované dôveryhodné služby, ktoré sa majú poskytovať, – certifikát pre každú príslušnú budúcu kvalifikovanú dôveryhodnú službu vydaný akreditovaným orgánom posudzovania zhody. * vzor formulára uverejní NBÚ na svojom webovom sídle a na ústrednom portáli verejnej správy

5.2 Požiadavky na kvalifikovaných a nekvalifikovaných poskytovateľov dôveryhodných služieb

Tabuľka T2

Identifikátor požiadavky	Požiadavka na kvalifikovaných a nekvalifikovaných poskytovateľov dôveryhodných služieb { možná realizácia požiadavky nariadenia }
Čl. 19 ods. 1 eIDAS	*Bezpečnosť dôveryhodných služieb:* TSP a QTSP vykonávajú posúdenie rizík pri identifikácii, analýze a hodnotení poskytovaných dôveryhodných služieb s prihliadnutím na obchodné problémy, technické problémy a technologický vývoj. Zvolia vhodnú elimináciu rizík použitím opatrení s prihliadnutím na výsledky posúdenia rizika. Príslušné technické a organizačné opatrenia zabezpečia, aby úroveň bezpečnosti bola primeraná predpokladanému riziku. Je potrené minimalizovať účinok bezpečnostných incidentov a informovať zainteresované strany o nepriaznivých účinkoch týchto incidentov. {**[8], [10],** ďalší návod je možné nájsť tiež v **[9]** }, v CS sú uvedené relevantné časti **[11] .**
Čl. 19 ods. 2 eIDAS	*Oznam o narušení bezpečnosti alebo integrity služieb:* TSP a QTSP sú bez zbytočného odkladu (najneskôr do 24 hod.), odkedy sa dozvedeli o akomkoľvek narušení bezpečnosti alebo integrity s významným vplyvom na poskytovanú dôveryhodnú službu alebo osobné údaje uchovávané v rámci dôveryhodnej služby, povinní oznámiť túto skutočnosť: – orgánu dohľadu, – prípadne iným príslušným orgánom: - vnútroštátny orgán zodpovedný za informačnú bezpečnosť, - orgán pre ochranu osobných údajov, – prípadne dotknutej fyzickej alebo právnickej osobe (ak môže narušenie bezpečnosti alebo integrity negatívne ovplyvniť túto fyzickú alebo právnickú osobu, ktorej sa poskytovala dôveryhodná služba), – verejnosti, ak o to poskytovateľa dôveryhodnej služby požiada informovaný orgán dohľadu vzhľadom na verejný záujem. **[11]** čl. 7.9

Tabuľka T3

Identifikátor požiadavky	Požiadavka na kvalifikovaných a nekvalifikovaných poskytovateľov dôveryhodných služieb { možná realizácia požiadavky nariadenia }
Čl. 13 ods. 1 a 2 eIDAS	*Poskytovatelia dôveryhodných služieb:* – *majú zodpovednosť za škodu, spôsobenú úmyselne alebo z nedbanlivosti akejkoľvek fyzickej alebo právnickej osobe tým, že nesplnia svoje povinnosti podľa eIDAS.* *Nekvalifikovaní poskytovatelia dôveryhodných služieb:* – *dôkazné bremeno týkajúce sa preukázania zodpovednosti nekvalifikovaného poskytovateľa dôveryhodných služieb za škodu spočíva na fyzickej alebo právnickej osobe, ktorá žiada o náhradu škody.* *Kvalifikovaní poskytovatelia dôveryhodných služieb:* – *škoda sa považuje za spôsobenú úmyselne alebo z nedbanlivosti, pokiaľ tento kvalifikovaný poskytovateľ dôveryhodných služieb nepreukáže opak, t. j. dôkazné bremeno spočíva na kvalifikovanom poskytovateľovi dôveryhodných služieb.* *Poskytovatelia dôveryhodných služieb:*

	– *ak svojim zákazníkom vopred riadne oznámia obmedzenia týkajúce sa využívania služieb, ktoré poskytujú, a ak tieto obmedzenia sú rozpoznateľné tretími stranami, poskytovatelia dôveryhodných služieb nenesú zodpovednosť za škody spôsobené využívaním služieb, ktorým sa takéto oznámené obmedzenia prekročili.* TSP a QTSP musia mať s ohľadom na riziko zodpovednosti za škodu k dispozícii dostatočné finančné zdroje alebo musia uzavrieť vhodné poistenie zodpovednosti za škody, v súlade s vnútroštátnymi právnymi predpismi, na krytie záväzkov vyplývajúcich z ich činností. *(čl. 24 ods. 2 písm. c) eIDAS),* **[11]**, 7.1.1 c) Zákazníci a strany závislé na dôveryhodných službách majú byť informovaní o presných podmienkach ešte pred vstupom do zmluvného vzťahu. Podmienky a pravidlá budú sprístupnené prostredníctvom komunikačných prostriedkov v ľahko zrozumiteľnom jazyku a môžu byť oznamované elektronicky. TSP a QTSP sprístupnia podmienky týkajúce sa poskytovania služieb všetkým účastníkom a závislým stranám. Tieto podmienky majú byť stanovené pre každú politiku dôveryhodných služieb nasledovne: a) aplikovanie politiky dôveryhodnej služby, b) všetky obmedzenia týkajúce sa poskytovaných služieb a zodpovednosti za ne, c) záväzky klientov, ak existujú, d) informácie pre zákazníkov spoliehajúcich sa na dôveryhodné služby, e) doba, počas ktorej sú uchovávané protokoly udalostí TSP a QTSP, f) obmedzenia týkajúce sa využívania služieb nad rámec stanovený príslušným obmedzením a zodpovednosť za náhradu škody, g) príslušný právny systém, h) postupy vybavovania sťažností a urovnávania sporov, i) kontaktné informácie o TSP a QTSP, j) záväzky v súvislosti so službami. V CS sú uvedené relevantné časti **[11]** , **[12]**.

5.3 Požiadavka na kvalifikovaných poskytovateľov dôveryhodných služieb

Tabuľka T4

Identifikátor požiadavky	Požiadavka na kvalifikovaných poskytovateľov dôveryhodných služieb { možná realizácia požiadavky nariadenia }
Čl. 20 ods. 1 eIDAS	*Podrobenie sa auditu zo strany orgánu posudzovania zhody aspoň raz za 24 mesiacov. Predloženie výslednej správy o posúdení zhody orgánu dohľadu v lehote troch pracovných dní od jej doručenia.* Správa o posúdení zhody (Conformity Assesment Report) musí byť vydaná akreditovaným orgánom posudzovania zhody a má potvrdiť, že QTSP spĺňajú podmienky poskytovania dôveryhodných služieb stanovené kritériami auditu v súlade s certifikačnou schémou.
Čl. 20 ods. 2 eIDAS	*Podrobenie sa auditu zo strany orgánu dohľadu alebo orgánu posudzovania zhody podľa požiadaviek orgánu dohľadu.* Orgán dohľadu určil certifikačnú schému záväznú pri výkone posudzovania zhody orgánom posudzovania zhody. Dodržiavanie certifikačnej schémy kontroluje pri akreditácii národný akreditačný orgán, ktorým je v Slovenskej republike SNAS.

	Orgán posudzovania zhody akreditovaný iným akreditačným orgánom v súlade s nariadením eIDAS musí aplikovať pri certifikácii QTSP platnú certifikačnú schému vydanú orgánom dohľadu http://ep.nbusr.sk/kca/tsl/CertifikacnaSchemaNBU.pdf V prípade využitia orgánu posudzovania zhody akreditovaného v zahraničí, musí mať tento orgán akreditáciu, ktorej pravidlá sú zodpovedajúce požiadavkám SNAS.

Tabuľka T5

Identifikátor požiadavky	Požiadavka na kvalifikovaných poskytovateľov dôveryhodných služieb { možná realizácia požiadavky nariadenia }
Čl. 24 ods. 1 až 4 eIDAS,	*Povinnosti kvalifikovaného poskytovateľa dôveryhodných služieb:* – *v súlade s vnútroštátnym právom overiť totožnosť prípadne ďalšie osobitné atribúty fyzickej alebo právnickej osoby, ktorej vydáva kvalifikovaný certifikát, (čl. 24 ods. 1 eIDAS).* QTSP musia overiť vhodnými prostriedkami a v súlade so ZDS totožnosť a prípadne ďalšie konkrétne atribúty fyzickej alebo právnickej osoby, ktorej bude (je) vydaný kvalifikovaný certifikát. Tieto informácie musia byť overené buď priamo, alebo spoliehaním sa na tretiu stranu v súlade s vnútroštátnymi právnymi predpismi: a) fyzická prítomnosť fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, alebo b) vzdialene pomocou prostriedkov elektronickej identifikácie, pričom pri prvotnej registrácii bola nutná prítomnosť fyzickej osoby alebo splnomocneného zástupcu právnickej osoby, c) pomocou kvalifikovaného certifikátu elektronického podpisu vydaného v súlade s bodom a) alebo b) alebo pomocou iných identifikačných metód uznávaných na národnej úrovni, ktoré poskytujú rovnakú záruku spoľahlivosti rovnocennú fyzickej prítomnosti. Tento ekvivalent má byť potvrdený orgánom posudzovania zhody. V CS sú uvedené relevantné časti **[12] a [13].** – *požiadavky na personál zamestnávaný kvalifikovaným poskytovateľom dôveryhodných služieb, (čl. 24 ods. 2 písm. b) eIDAS)* QTSP majú povinnosť zamestnávať zamestnancov a prípadne subdodávateľov, ktorí disponujú nevyhnutnou odbornosťou, spoľahlivosťou, skúsenosťou a kvalifikáciou a ktorí absolvovali príslušné školenie týkajúce sa bezpečnosti a pravidiel na ochranu osobných údajov a budú používať správne riadiace postupy, ktoré zodpovedajú európskej alebo medzinárodnej norme. – *udržiavať dostatočné finančné prostriedky alebo uzatvoriť poistenie zodpovednosti za škodu v súlade so slovenskou legislatívou v súvislosti s rizikom vzniku zodpovednosti za škodu, (čl. 24 ods. 2 písm. c) eIDAS)* QTSP musia mať s ohľadom na riziko zodpovednosti za škodu v súlade s článkom 13 eIDAS k dispozícii dostatočné finančné zdroje alebo musia uzavrieť vhodné poistenie zodpovednosti v súlade s vnútroštátnymi právnymi predpismi, – *pred uzatvorení zmluvného vzťahu je potrebné jednoznačne a vyčerpávajúco informovať každú osobu, ktorá chce využívať kvalifikovanú dôveryhodnú službu:*

	- *o presných podmienkach využívania tejto služby,* - *o obmedzeniach využívania tejto služby, (čl. 24 ods. 2 písm. d) eIDAS)* Konkrétne informácie o podmienkach poskytovania kvalifikovaných dôveryhodných služieb a súvisiacou zodpovednosťou sú uvedené v tabuľke T3. – *použitie dôveryhodných systémov a produktov, (čl. 24 ods. 2 písm. e) eIDAS)* QTSP musia používať dôveryhodné systémy a produkty, ktoré sú chránené proti pozmeňovaniu a musia zaistiť technickú bezpečnosť a spoľahlivosť procesov, ktoré podporujú {Príklad primeraného plnenia v ISO / IEC 27001: 2013 kap. A12, A 14, A15: a) analýza bezpečnostných požiadaviek musí byť navrhnutá v súvislosti s požiadavkami pre akúkoľvek fázu vývoja príslušných systémov. Projekt má byť realizovaný podľa návrhov QTSP alebo v ich mene, aby sa zaručilo, že je bezpečne navrhnutý do systémov IT, b) použijú sa kontrolné postupy na inštaláciu, modifikácie a havarijné opravy operačných systémov a softvérových prostriedkov vrátane zmien v konfigurácii pri uplatňovaní bezpečnostnej politiky QTSP. Postupy musia zahŕňať príslušnú dokumentáciu zmien , c) integrita informačných systémov QTSP musí byť chránená voči vírusom, škodlivým a neoprávneným softvérom, d) Informačné systémy QTSP používajúce úložné médiá pre poskytovanie príslušných služieb musia byť bezpečne chránené pred poškodením, krádežou a neoprávneným prístupom. e) postupy pre ochranu médií musia stanoviť ochranu proti starnutiu a zhoršeniu kvality v určenom časovom období, ktoré je potrebné na zachovanie potrebných záznamov, f) postupy musia byť zavedené pre všetky dôveryhodné a administratívne role, ktoré majú vplyv na poskytovanie služieb, g) QTSP musia stanoviť a uplatňovať postupy na zabezpečenie toho, aby: – bezpečnostné záplaty boli aplikované v primeranej lehote po tom, čo budú k dispozícii, – bezpečnostné záplaty neboli použité v prípade, že by vytvorili ďalšie zraniteľné miesta alebo nestability, ktoré prevážia prínos pri ich uplatnení, – dôvody, prečo neboli použité akékoľvek bezpečnostné záplaty majú byť zdokumentované. } – *použitie dôveryhodných systémov na uchovávanie poskytnutých údajov, (čl. 24 ods. 2 písm. f) eIDAS)* QTSP musia používať spoľahlivé dôveryhodné systémy na ukladanie údajov tak, aby: a) forma príslušných údajov bola overiteľná, b) údaje boli verejne prístupné iba po získaní súhlasu osoby, ktorej sa týkajú, c) bolo umožnené zadávať a uchovávať údaje len oprávneným osobám, d) bola daná možnosť kontroly údajov z hľadiska ich pravosti, e) boli prijaté vhodné opatrenia voči falšovaniu a krádeží údajov. – *prijatie vhodných opatrení proti falšovaniu a krádeží údajov, (čl. 24 ods. 2 písm. g) eIDAS)* QTSP majú kontrolovať fyzický prístup k systémom QTSP, ktorých bezpečnosť je rozhodujúca pre poskytované dôveryhodné služby, a minimalizovať riziká spojené s fyzickou bezpečnosťou.

	V CS sú uvedené relevantné časti **[11], [12].** {Príklad primeraného plnenia najmä ISO 27001:2013 kap. A11: a) fyzický prístup k systémom QTSP je obmedzený na oprávnené osoby, b) straty, poškodenia alebo ohrozenia majetku, odcudzenia informácií a zariadení, pričom nemá byť narušená prevádzka firmy, c) aby systémy, ktoré sú dôležité pre bezpečnú prevádzku dôveryhodnej služby boli umiestnené v chránenom bezpečnom priestore, d) aby bolo zamedzené vniknutie do priestorov prostredníctvom detekcie a poplachu v bezpečnostnom perimetri. } V CS sú uvedené relevantné časti **[11], [12].** – *spracúvanie osobných údajov v súlade s právnymi predpismi, (čl. 24 ods. 2 písm. j) eIDAS)* QTSP musia osobné údaje spracúvať a evidovať v súlade s vnútroštátnymi právnymi predpismi (**[3]** a primerane podľa smernice 95/46/ES **[6]**). **[12]** ods. 6.8.4. – *kvalifikovaný poskytovateľ dôveryhodných služieb, ktorý vydáva kvalifikované certifikáty: (čl. 24 ods. 2 písm. k), čl. 24 ods. 3 a 4 eIDAS)* QTSP zriaďuje a priebežne aktualizuje databázu certifikátov,**[12]** ods. 6.1, v prípade zrušenia certifikátu zaznamená takéto zrušenie vo svojej databáze certifikátov a uverejní štatút zrušenia certifikátu čo najskôr (max. do 24 hod od doručenia žiadosti), zrušenie nadobudne účinnosť okamžite po jeho zverejnení, **[12]** ods. 6.2.4, QTSP povinne poskytne informácie o štatúte platnosti alebo zrušenia kvalifikovaných certifikátov, ktoré vydal, každej spoliehajúcej sa strane, informácie o štatúte platnosti jednotlivých certifikátov sa poskytujú kedykoľvek, a to aj po uplynutí doby platnosti certifikátu, automatizovaným spôsobom, ktorý je spoľahlivý, bezplatný a efektívny, **[12]** ods. 6.2.4. – *záznamy relevantných informácií týkajúcich sa údajov, ktoré kvalifikovaný poskytovateľ dôveryhodných služieb vydal a prijal, (môže aj v elektronickej forme) a po primeranú dobu aj ich archiváciu (a to aj po ukončení činností kvalifikovaného poskytovateľa dôveryhodných služieb) najmä na účely:* *- zabezpečenia kontinuity služby,* *- predloženia dôkazov v súdnom konaní. (čl. 24 ods. 2 písm. h) eIDAS)* QTSP musia uvedené dostupné informácie zaznamenávať a uchovávať počas primeranej doby. Zodpovedajúce technické a organizačné opatrenia majú zabrániť neoprávnenému alebo nezákonnému spracovávaniu osobných údajov, ich náhodnej strate, zničeniu alebo poškodeniu: a) dôvernosť a integrita aktuálnych aj archívnych záznamov týkajúcich sa prevádzkovania služieb musí byť zachovaná, b) záznamy v súvislosti s prevádzkou služieb musia byť úplne a dôverne archivované v súlade so stanovenými obchodnými praktikami, c) záznamy týkajúce sa poskytovaných služieb sa majú archivovať počas určitej doby podľa potreby z dôvodu zaistenia nevyhnutných právnych dôkazov v súlade s bezpečnostnou politikou vydanou QTSP, d) presný čas významných udalostí v prostredí QTSP, správa kľúčov a čas synchronizácie udalostí musia byť zaznamenané. Doba zaznamenávania

	udalostí, ako je stanovené v protokole auditu, je synchronizovaná s koordinovaným svetovým časom (UTC) minimálne 1 x za 24 hodín s presnosťou minimálne 1s, e) informácie musia byť zaznamenávané takým spôsobom, že nemôžu byť ľahko odstránené alebo zničené (s výnimkou prípadov, keď sú spoľahlivo uložené na médiá, ktoré umožňujú dlhodobé uchovávanie v lehote, ktorá sa od nich vyžaduje). **[12]** ods. 6.3, 6.4 {*ISO 22301:2012*} – *informovať orgán dohľadu o všetkých zmenách pri poskytovaní kvalifikovaných dôveryhodných služieb a o zámere ukončiť tieto činnosti, (čl. 24 ods. 2 písm. a) eIDAS, § 6 ZDS)* – *aktualizovať plán ukončenia činností poskytovania služieb na zabezpečenie kontinuity služby v súlade s ustanoveniami overenými orgánom dohľadu podľa čl. 17. ods. 4 písm. i) nariadenia eIDAS. (čl. 24 ods. 2 písm. i) eIDAS, § 4 ods. 2 ZDS).* Potenciálne narušenia služieb poskytovaných zákazníkom a spoliehajúcim sa stranám musia byť minimalizované z dôvodu možného ukončenia týchto služieb. Predovšetkým je potrebné nepretržité uchovávanie informácií potrebných na overenie správnosti dôveryhodných služieb. **[11]** ods. 7.12, **[12]** ods. 6.4.9 QTSP musia mať aktuálny plán ukončenia činnosti, pričom sa uplatňujú tieto zásady: - povinnosť informovať o ukončení poskytovania služieb všetkých účastníkov a ostatné súvisiace subjekty, s ktorými majú QTSP zmluvy alebo inú formu zavedených vzťahov, kam patria QTSP, príslušné orgány dohľadu a ďalšie spoliehajúce sa strany, **[11]** ods. 7.12 - QTSP ukončí oprávnenosť všetkých subdodávateľov konať v ich mene pri výkone akýchkoľvek úloh týkajúcich sa poskytovania dôveryhodných služieb, **[11]** ods. 7.12 - pokiaľ je to možné, QTSP by mal zabezpečiť prenos poskytovania dôveryhodných služieb svojim klientom na iného QTSP**,** - QTSP prevedie svoje záväzky počas primeraného obdobia na spoľahlivého QTSP z dôvodu zachovania všetkých potrebných informácií ako dôkaz o činnosti QTSP, pričom musí zabezpečiť, aby súkromné kľúče vrátane záložných kópií boli zničené, alebo stiahnuté z používania, a to takým spôsobom, že súkromné kľúče už nie je možné opätovne získať, **[11]** ods. 7.12b iii, iv) - QTSP musia mať zmluvu z dôvodu pokrytia nákladov na splnenie minimálnych požiadaviek v prípade bankrotu, alebo neschopnosti pokryť náklady z iných dôvodov, ale v zmysle príslušných právnych predpisov týkajúcich sa bankrotu, **[11]** ods. 7.12c - QTSP majú mať vo svojich postupoch uvedené podmienky pre ukončenie prevádzky, ktoré obsahujú informácie o dotknutých subjektoch a prenesenie záväzkov na iných QTSP, **[11]** ods. 7.12d - QTSP majú povinnosť na primeraný čas sprístupniť svoj verejný kľúč alebo preniesť poskytovanie dôveryhodných služieb na spoľahlivý subjekt. **[11]** ods. 7.12e

Tabuľka T6

Identifikátor požiadavky	Požiadavka na kvalifikovaných poskytovateľov dôveryhodných služieb { možná realizácia požiadavky nariadenia }
Čl. 23 ods. 1 a 2 eIDAS, Vykonávacie nariadenie komisie 2015/806	*Kvalifikovaní poskytovatelia dôveryhodných služieb majú možnosť používať značku dôvery EÚ:* V prípade použitia značky dôvery EÚ: – používanie tejto značky je jasným označením kvalifikovaných dôveryhodných služieb odlišných od dôveryhodných služieb, – cieľom je posilniť dôveru a pohodlie používateľov, – značka prispieva k transparentnosti na trhu, pričom podporuje dôveru k využívaniu elektronických služieb, – podmienkou používania značky dôvery je, aby QTSP na svojom webovom sídle uviedli odkaz na dôveryhodný zoznam týkajúci sa poskytovania svojich kvalifikovaných dôveryhodných služieb. **[5]** čl. 4 ods. 1

Príloha A Oznámenie o zámere poskytovať kvalifikované dôveryhodné služby

Návrh obsahu formulára (listinná aj elektronická forma) v zmysle zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

Oznámenie o zámere poskytovať kvalifikované dôveryhodné služby

(§ 3 ods. 1 zákona č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov)

1. základné údaje (vyplní poskytovateľ dôveryhodných služieb)

Názov poskytovateľa dôveryhodných služieb:

Sídlo poskytovateľa dôveryhodných služieb:

Dátum predloženia oznámenia o zámere poskytovať kvalifikované dôveryhodné služby:

Právna forma podnikania poskytovateľa dôveryhodných služieb:

Identifikačné údaje poskytovateľa dôveryhodných služieb:

1. IČO:
2. DIČ:
3. IČ DPH: ☐ bezpredmetné
4. Bankový účet vo formáte IBAN:
5. BIC kód:
6. Zápis v OR (oddiel, vložka č.):

Údaje štatutárneho orgánu poskytovateľa dôveryhodných služieb:

1. Priezvisko, meno, titul:
2. Adresa:
3. Štátna príslušnosť:
4. Rodné číslo:
5. Deň vzniku funkcie:

Zámer poskytovať kvalifikované dôveryhodné služby:

Certifikáty budúcich kvalifikovaných dôveryhodných služieb:

☐ Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre elektronický podpis

☐ Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre elektronickú pečať

☐ Kvalifikovaná dôveryhodná služba vyhotovovania a overenia kvalifikovaných certifikátov pre autentifikáciu webových sídiel

☐ Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických podpisov

☐ Kvalifikovaná dôveryhodná služba validácie kvalifikovaných elektronických pečatí

☐ Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických podpisov

☐ Kvalifikovaná dôveryhodná služba uchovávania kvalifikovaných elektronických pečatí

☐ Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok

☐ Kvalifikovaná dôveryhodná elektronická doručovacia služba pre registrované zásielky

☐ Iná podriadená služba

Popis podriadenej služby:

2. Priložené dokumenty (vyplní poskytovateľ dôveryhodných služieb):

☐ 2.2 Doložený výpis z obchodného registra alebo doklad o oprávnení na vykonávanie podnikateľskej činnosti nie starší ako 3 mesiace P/E[1)]

- ☐ 2.2.1 platnosť
- ☐ 2.2.2 predmet činnosti

☐ 2.3 Výpis z registra trestov štatutárnych zástupcov právnickej osoby alebo z registra trestov fyzickej osoby nie starší ako 3 mesiace P/E[1)]

- ☐ 2.3.1 platnosť

☐ 2.4 Akreditačný orgán, vykonávajúci akreditáciu orgánov posudzovania zhody v EÚ *(http://www.european-accreditation.org/ea-members)*

- ☐ 2.4.1 Slovenská národná akreditačná služba (SNAS) *(čl. 3 ods. 18 eIDAS, nariadenie EP a R (ES) č. 765/2008, zákon č. 505/2009 Z. z.), EN ISO/IEC 17065:2013, ETSI EN 319403 v2.2.2 (2015-08)*
- ☐ 2.4.2 Zahraničný akreditačný orgán:
  Popis :

☐ 2.5 Správa o posúdení zhody dodaná poskytovateľom dôveryhodných služieb

☐ 2.6 Potvrdenie o zaplatení správneho poplatku *(položka 268 písm. a) sadzobníka správnych poplatkov podľa prílohy zákona č. 145/0995 Z. z.)*

☐ 2.7 Zverejňované údaje na webovom sídle: P/E[1)]

- ☐ 2.7.1 certifikačná politika
- ☐ 2.7.2 kvalifikované dôveryhodné služby (QTS)

- ☐ 2.7.3 používané technické špecifikácie, formáty a štandardy
- ☐ 2.7.4 cenník platených QTS a zoznam bezplatne poskytovaných QTS
- ☐ 2.7.5 obmedzenia pri poskytovaní QTS, ak existujú
- ☐ 2.7.6 spôsob overenia totožnosti žiadateľa o poskytnutie QTS
- ☐ 2.7.7 informácie o udelenom kvalifikovanom štatúte
  - ☐ 2.7.7.1 pridelený jednoznačný identifikátor kvalifikovanej dôveryhodnej služby vo formáte„TLIxx-y“ *(kap. 5.1.5 a 5.5.3 ETSI TS 119 612)*
- ☐ 2.7.8 URL adresa zverejňovaných informácií:
- ☐ 2.7.9 identifikačné údaje
- ☐ 2.7.10 informácie o vydaných kvalifikovaných certifikátoch
- ☐ 2.7.11 verejný kľúč TSP dostupný z viacerých informačných zdrojov

☐ 2.8 Zoznam príloh k oznámeniu o zámere poskytovať QTS P/E[1)]

☐ 2.9 Dokumentácia záznamov o poskytovaní QTS P/E[1)]
(čl. 24 písm. h eIDAS ,§ 5 ZDS)

☐ 2.10 Zoznam prevádzkovej dokumentácie TSP, pokiaľ nie je zverejnená na webovom sídle P/E[1)]

Zoznam:

Prípadné vysvetlenia (dôvod bezpredmetnosti a pod.)

3. Rozhodnutie (vyplní NBÚ):

☐ 3.1 Splnenie požiadaviek na oznámenie o zámere poskytovať QTS

☐ 3.2 Prerušenie konania o udelení kvalifikovaného štatútu P/E[1)]

☐ 3.3 Zamietnutie oznámenia o zámere poskytovať QTS a informovanie žiadateľa o poskytovanie QTS P/E[1)]

Vysvetlenie dôvodov:

Poznámka: Vyplnené polia: zaškrtnuté znamená „áno“, nevyplnené „nie“, prípadnú bezpredmetnosť treba zaškrtnúť a vysvetliť na konci dokumentu.

[1)] P - písomná forma, E - elektronická forma.

Príloha B História

Verzia	Dátum	Poznámka	Vypracoval
Verzia 1.0 Dr. 1	30.09.2016	Prvý návrh	Ing. Pavol Grünner, NBÚ Ing. Pavel Kubovič, NBÚ
Verzia 1.0	01.12.2016	Prvé vydanie	Ing. Pavol Grünner, NBÚ Ing. Pavel Kubovič, NBÚ
Verzia 2.0	28.02.2017	Druhé vydanie	Ing. Pavol Grünner, NBÚ Ing. Pavel Kubovič, NBÚ