



Verzia 0.3

Certifikačná schéma pre eIDAS

18.1.2017



Sekcia informačnej bezpečnosti a elektronického podpisu
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	4
2	Predmet dokumentu.....	4
3	Odkazy	5
4	Skratky	8
5	Predmet schémy	10
6	Požiadavky hodnotenia súladu.....	11
7	Aktivity primerané účelu a predmetu schémy.....	12
8	Ďalšie požiadavky na klienta auditu, ktoré musí splniť pri demonštrácii plnenia špecifických požiadaviek	12
9	Požiadavky na certifikačné orgány (CAB).....	12
10	Požiadavky na akreditáciu CAB.....	12
11	Metódy a postupy pri certifikácii.....	13
12	Informácie, ktoré má TSP dodať certifikačnému orgánu pri žiadosti o certifikáciu služieb podľa eIDAS..	13
13	Obsah certifikátu, ktorý jednoznačne identifikuje certifikované služby.....	13
14	Podmienky používania značky zhody a certifikátov	13
15	Zdroje.....	13
16	Správa z posúdenia	13
17	Nezhody.....	14
18	Postupy dohľadu	14
19	Prístup CAB a TSP k certifikačnej schéme	14
20	Podmienky zverejňovania certifikovaných služieb	15
21	Potreba a minimálny obsah zmlúv medzi CAB a klientom auditu (TSP).....	15
22	Spôsob overovania a vybavovania sťažností klientov auditu	15
23	Spôsob zverejňovania referencií na certifikáciu u klientov auditu.....	15
24	Doba uchovania záznamov u vlastníka schémy a CAB.....	15
25	Vzorkovanie	15
26	Akceptácia výsledkov iného posúdenia	15
27	Sťažnosti a odvolania ku vlastníkovi schémy	16
28	Licencia pre používanie certifikátov a certifikačných značiek.....	16
29	Nezhodné služby	16
30	Využívanie dodávateľov pri prevádzkovaní schémy.....	16
31	Využívanie CS v marketingu.....	16
32	Podvodné prezentovanie zhody.....	16
	Príloha A (normatívna) Kontrolný zoznam	17
	Príloha B História.....	18

1 Úvod

Certifikačnú schému posudzovania zhody (ďalej len „CS“) v zmysle eIDAS vydáva orgán dohľadu v súlade s EN ISO/IEC 17067:2013 ako vlastník schémy.

Upozornenie: CS podlieha povinnosti aktualizácie a bude priebežne dopĺňaná. Národný bezpečnostný úrad (ďalej len „NBÚ“) aktualizuje CS v nadväznosti na zmeny vo vykonávacích aktoch eIDAS a národnej legislatívy. V prípade rozporu medzi CS a vykonávacími aktami eIDAS resp. aktuálne platnou národnou legislatívou sa CS v spornom bode neaplikuje.

2 Predmet dokumentu

CS poskytuje orgánom posudzujúcim zhodu (ďalej len „CAB“) postup pri certifikácii dôveryhodných služieb podľa eIDAS. V záujme zachovania porovnateľnosti výstupov posudzovania zhody TSP stanovuje požiadavky s ohľadom na špecifické zameranie služieb poskytovaných TSP, pričom požiadavky ISO/IEC 17065: 2012 ako aj akreditačné požiadavky pre akreditáciu CAB zostávajú zachované.

Orgán dohľadu má v zmysle eIDAS ako aj ZDS právo požiadať CAB o vykonanie posúdenia zhody TSP alebo vlastného výkonu auditu, pričom vydáva CS pre zaistenie čo možno najvyššej objektívnosti posúdenia, prehľadnosti a porovnateľnosti výstupov posúdenia.

Súčasťou CS sú automaticky všetky dokumenty vydávané orgánom dohľadu pri výkone svojej úlohy v rámci eIDAS, ktoré zverejňuje NBÚ na svojom webovom sídle.

3 Odkazy

Odkazy na dokumenty, ktoré definujú použité typy a postupy.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. 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“).

[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] 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. Vykonávacie rozhodnutie Komisie (EÚ) 2015/1505 z 8. septembra 2015, ktorým sa ustanovujú technické špecifikácie a formáty týkajúce sa dôveryhodných zoznamov podľa článku 22 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (ďalej len „[Vykonávacie rozhodnutie Komisie \(EÚ\) 2015/1505](#)“).

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES ([všeobecné nariadenie o ochrane údajov](#)). Do 25.mája 2018 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] EN ISO/IEC 17067: 2013 Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes. Posudzovanie zhody – Základy certifikácie výrobkov a zásady pre schémy certifikácie výrobkov.

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

[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 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 dôveryhodných služieb.

[18] ENISA – Draft 0.4 – 11.2016 Guidelines for TSPs based on standards. Návod pre poskytovateľov 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 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 poskytovateľov dôveryhodných služieb. – Návod na posudzovanie zhody poskytovateľov dôveryhodných služieb.
- [21] Požiadavky na prevádzku kvalifikovaných poskytovateľov dôveryhodných služieb definované orgánom dohľadu (pozri <http://ep.nbusr.sk/kca/tsl/PoziadavkyPrevadzkyTSP.pdf>)
- [22] Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu (pozri <http://ep.nbusr.sk/kca/tsl/SchemaDohladu.pdf>)
- [23] ISO/IEC 17021-1: 2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements (ISO/IEC 17021-1: 2015). Posudzovanie zhody. Požiadavky na orgány vykonávajúce audit a certifikáciu systémov manažérstva. Časť 1: Požiadavky (ISO/IEC 17021-1: 2015).

4 Skratky

ASN.1	Abstract Syntax Notation 1
CA	Certifikačná autorita (Certification Authority) – poskytovateľ kvalifikovanej dôveryhodnej služby vyhotovovania a overovania kvalifikovaných certifikátov pre elektronický podpis, elektronickú pečať a pre autentifikáciu webových sídiel
CAB	Conformity Assessment Body (orgán posudzovania zhody).
CP	Certificate Policy (certifikačná politika)
CRL	Certificate Revocation List (zoznam zrušených certifikátov)
CS	Certifikačná schéma posudzovania zhody
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. 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 Európskej únie pre sieťovú a informačnú bezpečnosť) https://www.enisa.europa.eu/topics/trust-services
ISO	International Organization for Standardization (Medzinárodná organizácia pre normalizáciu)
NAB	National Accreditation Body (národný akreditačný orgán – SNAS)
NBÚ	Národný bezpečnostný úrad
OCSP	Online Certificate Status Protocol (protokol oznamovania stavu certifikátu online)
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)
SNAS	Slovenská národná akreditačná služba
TSA	Time-Stamping Authority (autorita časovej pečiatky)

TSP	Trust Service Provider (poskytovateľ dôveryhodných služieb)
UTC	Coordinated Universal Time (koordinovaný svetový čas)
ZDS	Zákon o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) Zákon č. 272/2016 Z. z.

5 Predmet schémy

CS sa týka posudzovania dôveryhodných služieb podľa eIDAS. V záujme zachovania porovnateľnosti výstupov posudzovania zhody TSP stanovuje požiadavky s ohľadom na špecifické zameranie služieb poskytovaných TSP, pričom požiadavky ISO/IEC 17065: 2012 ako aj akreditačné požiadavky pre akreditáciu CAB zostávajú zachované.

číslo	Názov produktu	Certifikačná schéma	Predpisy, normy
1	Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov <u>pre elektronický podpis</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 26, čl. 27, čl. 28, čl. 29, čl. 31 a Príloha I a II.
2	Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov <u>pre elektronickú pečať</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 29, čl. 31, čl. 36, čl. 37, čl. 38, čl. 39 a Príloha II a III.
3	Kvalifikovaná dôveryhodná služba vyhotovovania a overovania kvalifikovaných certifikátov <u>pre autentifikáciu webových sídiel</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 45 a Príloha IV.
4	Kvalifikovaná dôveryhodná služba validácie <u>kvalifikovaných elektronických podpisov</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 26, čl. 27, čl. 28, čl. 32, čl. 33
5	Kvalifikovaná dôveryhodná služba validácie <u>kvalifikovaných elektronických pečatí</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 32, čl. 33, čl. 36, čl. 37, čl. 38, čl. 40
6	Kvalifikovaná dôveryhodná služba uchovávanía <u>kvalifikovaných elektronických podpisov</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 34 a voliteľne služby č. 4
7	Kvalifikovaná dôveryhodná služba uchovávanía <u>kvalifikovaných elektronických pečatí</u>	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 34, čl. 40 a voliteľne služby č. 5
8	Kvalifikovaná dôveryhodná služba vyhotovovania kvalifikovaných elektronických časových pečiatok	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 42
9	Kvalifikovaná dôveryhodná elektronická doručovacia služba pre registrované zásielky	Certifikačná schéma NBÚ	Nariadenie (EU) č. 910/2014: Čl. 5, čl. 8, čl. 11 ods. 3, čl. 13, čl. 15, čl. 17 ods. 5, čl. 19, čl. 21, čl. 22, čl. 23, čl. 24, čl. 44

6 Požiadavky hodnotenia súladu

Požiadavky na TSP pri prezentovaní zhody pri plnení požiadaviek potrebných na získanie kvalifikovaného štatútu obsahujú nasledovné dokumenty:

- 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.
- [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).
- Požiadavky na prevádzku poskytovateľov dôveryhodných služieb definované orgánom dohľadu [22] vrátane uvádzaných odkazov na technické štandardy umožňujúce naplniť špecifické požiadavky, vid'. predovšetkým relevantné časti [11], [12], [13] a [15].
- Schéma dohľadu kvalifikovaných dôveryhodných služieb definovaná orgánom dohľadu vrátane uvádzaných odkazov na technické štandardy umožňujúce naplniť špecifické požiadavky, vid'. predovšetkým relevantné časti [11], [12], [13] a [15].
- 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.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 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.
- Vykonávacie rozhodnutia a nariadenia eIDAS (napr. na <http://www.nbu.gov.sk/urad/pravne-predpisy/doveryhodne-sluzby/index.html>)
- Certifikačná politika pre koreňovú CA a dôveryhodnú službu vyhotovovania kvalifikovaných certifikátov, ktorej kvalifikovaný štatút udelil Národný bezpečnostný úrad (platnosť od 01.11.2016) (http://ep.nbusr.sk/kca/doc/kcaq_cp1_2_2_v4_2016_9_21.pdf)
- Certifikačné a podpisové politiky zverejňované na webovom sídle orgánu dohľadu.

7 Aktivity primerané účelu a predmetu schémy

Výber predmetu(-ov) posudzovania zhody, vrátane výberu špecifikovaných požiadaviek, ktoré sa majú posudzovať, a plánovania zberu informácií a činností odberu vzoriek:

Certifikačný orgán postupuje pri výbere posudzovaných činností a plánovaní zberu informácií v súlade s ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015 . Predmetom certifikácie sú služby uvedené v kapitole 5. Klient auditu (TSP) nemusí vykonávať všetky služby, rozsah požadovanej certifikácie uvádza pri žiadosti o certifikáciu.

Určenie metód hodnotenia (napr. skúška, audit a/alebo preskúšanie) na získanie kompletných informácií ohľadne plnenia stanovených požiadaviek je predmetom posudzovania zhody alebo jeho vzorkou:

Pri certifikácii služieb podľa eIDAS sa vykonávajú hodnotenia súladu formou auditu. Certifikačný orgán pri výkone auditu postupuje v súlade s ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015.

Preskúmanie a osvedčenie, vrátane preskúmania dôkazu z etapy určovania a následné osvedčenie, že predmet posudzovania zhody spoľahlivo preukázal plnenie stanovených požiadaviek a následné označenie alebo licencovanie a súvisiace kontroly, tam kde je to relevantné sa vykonáva v súlade s ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015 .

Dohľad, vrátane frekvencie a rozsahu činností dohľadu a opätovného posúdenia, aby sa zabezpečilo, že predmet posudzovania zhody naďalej plní stanovené požiadavky: požiadavky na dohľad sú uvedené v príslušnej kapitole CS.

8 Ďalšie požiadavky na klienta auditu, ktoré musí splniť pri demonštrácii plnenia špecifických požiadaviek

Nie sú.

9 Požiadavky na certifikačné orgány (CAB)

Certifikačný orgán okrem podmienok vyplývajúcich z toho, že podlieha akreditácii (viď. ďalšia kapitola) musí rešpektovať požiadavky orgánu dohľadu, ktoré ukladá TSP v rámci svojho výkonu. Pri podávaní správ z posúdenia zhody TSP musí byť z výsledkov posúdenia možné rozhodnúť ohľadom splnenia podmienok pre kvalifikovaný štatút, k čomu je nevyhnutné predložiť dostatočne jednoznačnú správu z posúdenia zhody (viď kapitola 16).

10 Požiadavky na akreditáciu CAB

CAB podliehajú požiadavke akreditácie v zmysle ISO/IEC 17065: 2012 pre oblasť dôveryhodných služieb podľa eIDAS. Akreditačné postupy a podmienky akreditácie uvádza NAB na svojom webovom sídle www.snas.sk.

11 Metódy a postupy pri certifikácii

Pre zachovanie integrity a porovnateľnosti výstupov posúdenia špecifikuje táto schéma predovšetkým minimálny rozsah výstupov posúdenia vzhľadom na špecifiká certifikovaných služieb. Všetky požiadavky ISO/IEC 17065: 2012 a relevantných častí ISO/IEC 17021-1: 2015 sú zachované.

12 Informácie, ktoré má TSP dodať certifikačnému orgánu pri žiadosti o certifikáciu služieb podľa eIDAS

Rozsah informácií, ktoré má TSP dodať certifikačnému orgánu pri žiadosti o certifikáciu, stanovujú CAB pre svojich klientov v zmluvných dokumentoch v súlade s príslušnými ustanoveniami [7] a [14] ako aj v súlade s ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015.

13 Obsah certifikátu, ktorý jednoznačne identifikuje certifikované služby

Pre každú certifikovanú službu vydáva certifikačný orgán samostatný certifikát s uvedenou certifikačnou službou. Certifikovať možno služby s uvedením zhody v zmysle bodu 5.

14 Podmienky používania značky zhody a certifikátov

Podmienky používania značky certifikačného orgánu a certifikátov stanovujú CAB pre svojich klientov v zmluvných dokumentoch v súlade s príslušnými ustanoveniami [7] a [14] ako aj v súlade s ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015. Špecifické požiadavky na používanie značky dôvery pre TSP stanovuje eIDAS a ZDS.

15 Zdroje

Zdroje vyžadované pre prevádzku vrátane nezávislosti a kompetentnosti personálu (interného aj externého), zdrojov pre hodnotenie a využívania subdodávateľov musí CAB zabezpečiť minimálne na úrovni vyžadovanej v rámci [7] a [14] ako aj v súlade s ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015.

Zdroje TSP pri zabezpečovaní činností musia byť v súlade s požiadavkami na posudzované poskytované služby.

16 Správa z posúdenia

Podávanie správ o výsledkoch hodnotenia jednotlivých stupňov posúdenia, obsah správy a poskytovanie správy orgánu dohľadu stanovujú príslušné ustanovenia [7] a [14]. V zmysle nariadenia eIDAS ako aj ZDS odovzdáva správu z posúdenia orgánu dohľadu do 3 dní po doručení TSP.

Minimálny rozsah informácií v rámci správy z posúdenia musí umožniť orgánu dohľadu vyhodnotiť, či TSP plní požiadavky na získanie kvalifikovaného štatútu. Z tohto dôvodu musí CAB v rámci výstupov z posúdenia – či už ako súčasť správy alebo v rámci jej príloh – vyhodnotiť požiadavky minimálne v rozsahu podrobnosti uvedenej v kontrolnom zozname v Prílohe A. Kontrolný zoznam je pomôckou pre certifikačné orgány, ktorého účelom je zachytiť všetky

relevantné požiadavky na TSP v súlade s legislatívou, národnými rozšíreniami národnej dôveryhodnej infraštruktúry a požiadavkami národného orgánu dohľadu. V prípade potreby aktualizácie kontrolného zoznamu z dôvodu doplnenia požiadaviek v rámci európskej alebo národnej legislatívy vrátane požiadaviek orgánu dohľadu, prípadne pri zmene referencovaných štandardov, je certifikačný orgán povinný pri posudzovaní zhody doplniť aktualizované požiadavky do výstupov z posúdenia v súlade s aktuálnym stavom v čase posúdenia, ak by Príloha A nebola aktuálna.

Výstup z posúdenia v rámci hodnotenia súladu musí predovšetkým:

- sloвне a jednotlivo za každý článok vyhodnotiť súlad s požiadavkami uvedenými pre jednotlivé hodnotené služby v kapitole 5. Vyhlásenia o zhode s požiadavkami je potrebné uvádzať spolu so súhrnom dôkazov týkajúcich sa plnenia požiadaviek a pre každú hodnotenú službu je potrebné uviesť záver k vhodnosti rozsahu certifikácie. **V prípade, kedy nie je možné konštatovať zhodu s požiadavkami, nie je možné vydať certifikát o zhode služby.** Postup riešenia nezhôd stanovujú príslušné ustanovenia [7] a [14] ako aj ISO/IEC 17065: 2012 a pre audit relevantné časti ISO/IEC 17021-1: 2015.
- vyhodnotiť súlad s požiadavkami ZDS [2], ktoré obsahujú požiadavky na TSP (príklad kontrolného zoznamu s relevantnými požiadavkami obsahuje Príloha A)
- vyhodnotiť súlad s požiadavkami národného orgánu dohľadu [21] a [22] vrátane odkazovaných medzinárodných štandardov, ktoré orgán dohľadu určil ako povinné alebo ktoré TSP využíva dobrovoľne ako spôsob plnenia požiadaviek nad rámec povinných štandardov určených orgánom dohľadu, pričom vyhodnotenie súladu pre štandardy, ktorými preukazuje TSP zhodu s požiadavkami, je potrebné zdokumentovať minimálne na úrovni podrobnosti porovnateľnej s úrovňou v kontrolnom zozname v Prílohe A, pričom je CAB povinný v prípade potreby doplniť kontrolný zoznam pre ďalšie posudzované štandardy.

Dokumentovanie hodnotenia musí okrem vyššie uvedeného obsahovať predovšetkým záznam o preskúmaných dôkazoch s uvedením konkrétnych dôkazov, vzoriek, ich počtu a použitých metód pri hodnotení v podrobnosti ilustrovanej v Prílohe č. 1 na úrovni každého riadku, kde je to relevantné a možné. Príslušné ustanovenia [7] a [14] pre zaznamenávanie výsledkov hodnotenia musia byť zachované.

17 Nezhody

Postup pri zistení a riešení nezhôd s certifikačnými požiadavkami vrátane nezhody dôveryhodných služieb stanovujú príslušné ustanovenia [7] a [14] ako aj ISO/IEC 17065: 2012 a pre audit relevantné časti ISO/IEC 17021-1: 2015.

18 Postupy dohľadu

Pre výkon dohľadu z pohľadu frekvencie auditu, určenia frekvencie dozorných auditov vykonávaných CAB platia príslušné ustanovenia [7] a [14].

19 Prístup CAB a TSP k certifikačnej schéme

CS je verejný dokument, ktorý zverejňuje orgán dohľadu na svojom webovom sídle.

20 Podmienky zverejňovania certifikovaných služieb

V zmysle eIDAS orgán dohľadu vedie dôveryhodný zoznam, do ktorých zapisuje TSP, ktorý získal kvalifikovaný štatút po splnení podmienok uvedených v ZDS a súvisiacich predpisoch.

Zoznam certifikovaných subjektov a ich služieb uvádza CAB na svojom webovom sídle, pričom uvádza aj dátum zrušenia certifikátu podľa kapitoly 29.

21 Potreba a minimálny obsah zmlúv medzi CAB a klientom auditu (TSP)

Všeobecné podmienky pre udeľovanie, udržiavanie, pokračovanie, rozširovanie alebo zužovanie predmetu certifikácie, pozastavovanie a odoberanie certifikácie vrátane podmienky stiahnutia reklamy a vrátenia certifikačných dokumentov alebo akýchkoľvek nutných krokov, ak je certifikácia pozastavená, odobratá alebo ukončená realizuje CAB v súlade s aplikovateľnými ustanoveniami [7] a [14].

22 Spôsob overovania a vybavovania sťažností klientov auditu

Sťažnosti klienta auditu na CAB spracováva CAB v súlade s aplikovateľnými ustanoveniami [7] a [14]. Sťažnosti TSP vo vzťahu k orgánu dohľadu upravuje ZDS.

23 Spôsob zverejňovania referencií na certifikáciu u klientov auditu

Nie sú dodatočné požiadavky.

24 Doba uchovania záznamov u vlastníka schémy a CAB

Nie sú dodatočné požiadavky (určuje to ZDS a eIDAS).

25 Vzorkovanie

CAB musí pri vzorkovaní dodržiavať príslušné požiadavky ISO/IEC 17065: 2012 a relevantné časti ISO/IEC 17021-1: 2015 v súlade s aplikovateľnými ustanoveniami [7] a [14]. Vzorkovanie musí v dostatočnej miere umožniť spoľahlivé posúdenie pre výrok audítora minimálne v rozsahu požadovaných výstupov z posúdenia (viď. kapitola 16).

26 Akceptácia výsledkov iného posúdenia

CAB môže pri stanovovaní potrebného času pre výkon auditu (posúdenia zhody) prihliadať na predchádzajúce posúdenia alebo výsledky hodnotení (certifikácie) relevantné pre čiastkové plnenie požiadaviek (napr. ISO 27 001 pri plnení všeobecných požiadaviek na systém bezpečnosti) avšak táto certifikácia nemôže byť využitá ako náhrada výkonu hodnotenia špecifických požiadaviek pre certifikované služby a CAB musí dodržať potrebný rozsah hodnotenia v súlade s CS ako aj

ustanoveniami uvedenými a referencovanými v [7] a [14] a v súlade s akreditačnými požiadavkami na CAB.

27 Sťažnosti a odvolania ku vlastníkovi schémy

Sťažnosti na CAB majú byť adresované najprv na CAB v súlade s aplikovateľnými ustanoveniami [7] a [14] ako aj ISO/IEC 17065: 2012 a relevantnými časťami ISO/IEC 17021-1: 2015. Postup pri odvolaniach k vlastníkovi schémy stanovuje ZDS.

28 Licencia pre používanie certifikátov a certifikačných značiek

CAB musí pre stanovenie podmienok licencovania a používania vlastných certifikátov dodržiavať príslušné požiadavky ISO/IEC 17065: 2012 a relevantné časti ISO/IEC 17021-1: 2015 v súlade s aplikovateľnými ustanoveniami [7] a [14]. Postup pri používaní značky dôvery stanovuje eIDAS a ZDS.

29 Nezhodné služby

V prípade, že TSP viac neplní požiadavky, CAB postupuje v súlade s aplikovateľnými ustanoveniami [7] a [14] o pozastavení alebo odobratí certifikátu. TSP je povinný okamžite informovať orgán dohľadu o tejto skutočnosti v súlade s požiadavkami legislatívy [1], [2] a nesmie poskytovať služby, ktoré vyžadujú kvalifikovaný štatút.

30 Využívanie dodávateľov pri prevádzkovaní schémy

Vlastníkom CS je NBÚ ako orgán dohľadu určený v ZDS. V prípade využívania dodávateľov v rámci prevádzkovania CS určí orgán dohľadu podmienky formou metodiky alebo štandardu.

31 Využívanie CS v marketingu

CS nemá dodatočné požiadavky na politiky a procedúry súvisiace s marketingom a odkazovaním CAB a TSP na CS nad rámec postupov uvedených v iných odkazoch.

32 Podvodné prezentovanie zhody

V prípade, že TSP prezentuje zhodu s požiadavkami, pričom mu nebol udelený certifikát pre poskytované služby alebo mu nebol pre poskytovanie služieb udelený kvalifikovaný štatút, postupuje orgán dohľadu v zmysle sankcií uvedených v ZDS.

Príloha A (normatívna) Kontrolný zoznam

Kontrolný zoznam pozostáva z prvých dvoch hlavných hárkov a niekoľkých doplnkových hárkov pridávaných na základe potreby spresnenia plnenia povinných požiadaviek z prvých dvoch hárkov v dokumente "[checklistAuditTSP.xlsx](#)".

Príloha B História

Verzia	Dátum	Poznámka	Vypracoval
Verzia 0.3 Č.: 1354/2017/IBEP/OA-001	18.1.2017		