Literatura:
ENISA. *Analysis of standards related to Trust Service Providers Mapping of requirements of eIDAS to existing standards* [online]. Heraklion, Greece: ENISA, 2015. Citace 1. 11. 2020. Dostupné z: <https://www.enisa.europa.eu/publications/tsp_standards_2015>.
MINISTERSTVO VNITRA, *Metodika Ministerstva vnitra*.Praha: Ministerstvo vnitra, 2016.

Oddíl 7
Služba elektronického doporučeného doručování

Článek 43
Právní účinek služby elektronického doporučeného doručování

1. Datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování nesmějí být upírány právní účinky a nesmějí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nesplňují požadavky na kvalifikovanou službu elektronického doporučeného doručování.
2. U dat odeslaných a přijatých prostřednictvím kvalifikované služby elektronického doporučeného doručování platí domněnka integrity dat, odeslání těchto dat identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a správnosti data a času odeslání a přijetí, jež jsou u kvalifikované služby elektronického doporučeného doručování uvedeny.

Bod odůvodnění: 66.

Přehled výkladu:
I. Služba elektronického doporučeného doručování
II. Právní účinky služby elektronického doporučeného doručování

I. Služba elektronického doporučeného doručování

Službou elektronického doporučeného doručování se podle článku 3 odst. 36 Nařízení rozumí služba, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn. Nařízení rozlišuje **dvě úrovně důvěryhodnosti** této služby vytvářející důvěru pro elektronické transakce.

– První úrovní je služba elektronického doporučeného doručování bez přívlastku, na niž kromě definice, že musí zahrnovat nejen elektronické doručování, ale také poskytovat důkazy o tomto doručování a chránit přenášená data před rizikem ztráty, odcizení, poškození nebo neoprávněných změn, nejsou kladeny žádné konkrétní požadavky. Nicméně již uvedená zajištění jsou poměrně silná, takže např. běžná e-mailová komunikace tyto záruky v žádném případě nedává.
– Druhou úrovní je kvalifikovaná služba elektronického doporučeného doručování, která kromě výše uvedených vlastností musí dále splňovat požadavky článku 44 Nařízení, což

mimo jiné znamená, že musí být poskytována jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru jako kvalifikovaná služba vytvářející důvěru. Součástí této kvalifikované služby musí být zajištění dalších požadavků, jako je vysoká úroveň spolehlivosti identifikace odesílatele, zajištění identifikace příjemce před doručením dat, zabezpečení odesílání a přijímání dat prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat, vyrozumění odesílatele a příjemce v případě, kdy je potřeba změnit data za účelem jejich odeslání nebo přijetí, a v neposlední řadě označení data a času odeslání a přijetí, popř. též případné nezbytné změny dat, prostřednictvím kvalifikovaného elektronického časového razítka.

II. Právní účinky služby elektronického doporučeného doručování

Právní účinky služby elektronického doporučeného doručování se liší podle úrovně důvěryhodnosti diskutované výše.

– Podle článku 43 odst. 1 Nařízení nesmějí být datům odeslaným a přijatým prostřednictvím služby elektronického doporučeného doručování upírány právní účinky a nesmějí být odmítána jako důkaz v soudním a správním řízení pouze z toho důvodu, že mají elektronickou podobu nebo že nesplňují požadavky na kvalifikovanou službu elektronického doporučeného doručování. To znamená, že i nejnižší úroveň důvěryhodnosti elektronického doporučeného doručování musí být v každém konkrétním případě posuzována, pokud jsou data přenesená tímto systémem předkládána jako důkaz v soudním a správním řízení, byť míra důkazní spolehlivosti zde bude záviset na konkrétním technickém a procesním řešení. Avšak je třeba si uvědomit, že tato služba musí již v základu poskytovat důkazy o nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí těchto dat. Znamená to, že míra důkazní spolehlivosti zde není předjímána Nařízením, ale závisí případně na vnitrostátní právní úpravě, která se pak ale samozřejmě týká jen konkrétního členského státu.
  Definici služby elektronického doporučeného doručování jednoznačně naplňují datové schránky podložené zákonem o elektronických úkonech. Avšak nenaplňují podmínky kladené na kvalifikovanou službu elektronického doporučeného doručování, a proto nejsou kvalifikovanou službou elektronického doporučeného doručování (Lechner, Mitwallyová, 2017, s. 187 a násl.). Přesto jejich důvěryhodnost a schopnost prokazovat odeslání, dodání a doručení elektronického dokumentu v podobě datové zprávy je v rámci ČR velmi vysoká, tedy má vysokou míru důkazní spolehlivosti. Pokud by však byly tyto důkazy předloženy v rámci jiného členského státu, mohly by být na základně Nařízení posuzovány jen podle článku 43 odst. 1.
– Podle článku 43 odst. 2 Nařízení **platí u dat odeslaných a přijatých prostřednictvím kvalifikované služby elektronického doporučeného doručování domněnka integrity dat, odeslání těchto dat identifikovaným odesílatelem, jejich přijetí identifikovaným příjemcem a správnost data a času odeslání a přijetí, jež jsou u kvalifikované služby elektronického doporučeného doručování uvedeny**. Ačkoliv to Nařízení explicitně nestanoví, tak z principu jeho celoevropské platnosti lze toto ustanovení aplikovat i v přeshraničním užití kvalifikované služby elektronického doporučeného doručování, což zdůrazňuje i bod 66 odůvodnění Nařízení, kde se praví, že právní úprava kvalifikované služby elektronického doporučeného doručování je

součástí Nařízení z důvodu usnadnění přeshraničního uznávání služeb elektronického doporučeného doručování mezi stávajícími vnitrostátními právními systémy.

V ČR v současné době neexistuje žádná kvalifikovaná služba elektronického doporučeného doručování splňující požadavky Nařízení. Podle aktuálních důvěryhodných seznamů vedených a zveřejňovaných dle článku 22 jednotlivými členskými státy je aktuálně v EU nabízeno 20 kvalifikovaných služeb elektronického doporučeného doručování v šesti státech.

Související ustanovení:
čl. 3 odst. 36 – Definice, čl. 44 – Požadavky na kvalifikované služby elektronického doporučeného doručování

Související předpisy:
zák. o elektronických úkonech

Literatura:
LECHNER, T., MITWALLYOVÁ, H. Legal Analysis of the Development of Data Mailboxes in the Context of the eIDAS Regulation. In VAŇKOVÁ, I. (ed.) *Proceedings of the 12th International Scientific Conference*, Public Economics and Administration 2017. Ostrava: VŠB – Technical University of Ostrava, 2017.

Článek 44

Požadavky na kvalifikované služby elektronického doporučeného doručování

1. **Kvalifikované služby elektronického doporučeného doručování musí splňovat tyto požadavky:**
   a) **jsou poskytovány jedním či více kvalifikovanými poskytovateli služeb vytvářejících důvěru;**
   b) **s vysokou úrovní spolehlivosti zajišťují identifikaci odesílatele;**
   c) **zajišťují identifikaci příjemce před doručením dat;**
   d) **odesílání a přijímání dat je zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru tak, aby byla vyloučena možnost nezjistitelné změny dat;**
   e) **odesílatel a příjemce dat jsou jednoznačně vyrozuměni o případných změnách dat potřebných za účelem odeslání nebo přijetí dat;**
   f) **datum a čas odeslání, přijetí a případná změna dat jsou označeny prostřednictvím kvalifikovaného elektronického časového razítka.**

   V případě přenosu dat mezi dvěma či více kvalifikovanými poskytovateli služeb vytvářejících důvěru se požadavky uvedené v Písm. a) až f) vztahují na všechny tyto kvalifikované poskytovatele služeb vytvářejících důvěru.
2. **Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro postupy odesílání a přijímání dat. Pokud postup odesílání a přijímání dat vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v odstavci 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.**

Bod odůvodnění: 66.

Kvalifikovaná služba elektronického doporučeného doručování

Aby mohla být kvalifikovaná služba elektronického doporučeného doručování spojena s mnohými domněnkami, jak to uvádí článek 43 odst. 2 Nařízení, musí splnit celou řadu pravidel. Základní pravidla jsou dána článkem 44 odst. 1, přičemž v případě přenosu dat mezi dvěma či více kvalifikovanými poskytovateli služeb vytvářejících důvěru musejí všechny uvedené požadavky splnit všichni zapojení poskytovatelé. Podle odstavce 2 může Komise prostřednictvím prováděcích aktů určit referenční čísla norem pro postupy odesílání a přijímání dat touto službou, avšak dosud žádný takový předpis vydán nebyl. A tedy jediné, o co se lze po technické stránce opřít, jsou doporučení agentury ENISA, která se vyjadřují k jednotlivým požadavkům odstavce 1 a která většinou odkazují na normu ETSI TS 102 640 V2.1.1 (2010-01): *„Electronic Signatures and Infrastructures (ESI): Registered Electronic Mail (REM)"* (ENISA, 2015, s. 59-60).

- Kvalifikovaná služba elektronického doporučeného doručování může být poskytována pouze kvalifikovaným poskytovatelem služeb vytvářejících důvěru, přičemž se nevylučuje zřetězení těchto služeb, ani vzájemná spolupráce těchto poskytovatelů. Nicméně stanovená pravidla musí splnit každý z nich. Podle citovaného dokumentu agentury ENISA se standardy vzájemnými vazbami mezi kvalifikovanými službami elektronického doporučeného doručování nezabývají.
- Kvalifikovaná služba elektronického doporučeného doručování musí s vysokou úrovní spolehlivosti zajišťovat identifikaci odesílatele, přičemž zde není žádné omezení, zda odesílatelem může být fyzická osoba, právnická osoba nebo fyzická osoba zastupující právnickou osobu. Požadavek vysoké úrovně spolehlivosti není „mapován" na úrovni záruky systémů elektronické identifikace podle článku 8 Nařízení, i když lze předpokládat přímočaré propojení identifikace odesílatele na elektronickou identifikaci dle Nařízení. Ukazuje se zde opět již několikrát zmíněná oddělenost dvou částí Nařízení popisujících elektronickou identifikaci a služby vytvářející důvěru pro elektronické transakce (Kment, 2018, s. 108), která v tomto případě působí až kontraproduktivně.
- Kvalifikovaná služba elektronického doporučeného doručování musí zajistit identifikaci příjemce před doručením dat. Tento požadavek nejen zajišťuje identifikaci příjemce jako takovou, ale jeho formulace „před doručením" zároveň znamená ochranu doručovaných dat, aby se s jejich obsahem nemohl seznámit nikdo jiný než adresát. Jde tedy o jistou formu zajištění listovního tajemství. V rámci normy TS 102 640 je tento bod zahrnut do funkčního zajištění protokolu.
- Stejně jako kvalifikovaný certifikát pro elektronický podpis anebo kvalifikovaný certifikát pro elektronickou pečeť musí obsahovat zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává, tak odesílání a přijímání dat prostřednictvím kvalifikované služby elektronického doporučeného doručování musí být zabezpečeno prostřednictvím zaručeného elektronického podpisu nebo zaručené elektronické pečeti kvalifikovaného poskytovatele služeb vytvářejících důvěru a to ještě tak, aby byla vyloučena možnost nezjistitelné změny dat.
- Pokud je třeba za účelem odeslání nebo přijetí dat změna těchto dat, musí o tom být v rámci poskytování kvalifikované služby elektronického doporučeného doručování odesílatel a příjemce jednoznačně vyrozuměni. Podle citovaného dokumentu agentury ENISA odkazovaná norma TS 102 640 vylučuje jakoukoliv změnu dat.

– Kvalifikovaná služba elektronického doporučeného doručování musí zajistit, aby datum a čas odeslání dat, datum a čas přijetí dat a datum a čas případné změny dat byly stvrzeny použitím kvalifikovaného elektronického časového razítka. To podle citovaného dokumentu agentury ENISA není dosud v odkazovaném standardu aplikováno, neboť již realizované systémy elektronického doporučeného doručování (nikoliv poskytované jako kvalifikovaná služba vytvářející důvěru) mají vlastní implementace prokazování data a času.

Související ustanovení:
čl. 43 odst. 2 – Právní účinek služby elektronického doporučeného doručování

Literatura:
ENISA. *Analysis of standards related to Trust Service Providers Mapping of requirements of eIDAS to existing standards* [online]. Heraklion, Greece: ENISA, 2015. Citace 1. 11. 2020. Dostupné z: <https://www.enisa.europa.eu/publications/tsp_standards_2015>.
KMENT, V. *Elektronické právní jednání*. Praha: Wolters Kluwer, 2018.

Oddíl 8
Autentizace internetových stránek

Článek 45
Požadavky na kvalifikované certifikáty pro autentizaci internetových stránek

1. Kvalifikované certifikáty pro autentizaci internetových stránek musí splňovat požadavky stanovené v příloze IV.
2. Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikované certifikáty pro autentizaci internetových stránek. Pokud kvalifikovaný certifikát pro autentizaci internetových stránek vyhovuje těmto normám, předpokládá se shoda s požadavky stanovenými v příloze IV. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 48 odst. 2.

Bod odůvodnění: 67.

Kvalifikované certifikáty pro autentizaci internetových stránek

Kromě kvalifikovaných certifikátů pro elektronický podpis nebo elektronickou značku zavádí Nařízení též kvalifikované certifikáty pro autentizaci internetových stránek. Jejich poskytování i využívání je zcela dobrovolné, jak též zdůrazňuje bod 67 odůvodnění Nařízení. Ani v ČR není žádným zákonem zavedena povinnost využití těchto kvalifikovaných certifikátů, a to ani subjekty veřejného sektoru, u kterých by mohlo být povinné využití ku prospěchu zvýšení důvěryhodnosti postupující elektronizace veřejné správy (srov. zákon o právu na digitální služby).

Podle článku 3 odst. 38 Nařízení se certifikátem pro autentizaci internetových stránek rozumí potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán. Kvalifikovaný certifikát pro autentizaci

internetových stránek musí být navíc vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a musí splňovat požadavky stanovené v příloze IV (viz článek 3 odst. 39 a čl. 45 odst. 1). Podle článku 45 odst. 2 může Komise prostřednictvím prováděcích aktů určit referenční čísla norem pro kvalifikované certifikáty pro autentizaci internetových stránek, avšak dosud nebyl žádný takový předpis vydán. Doporučení agentury ENISA uvádí jako vhodnou normu ETSI EN 319 412-4 *„Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates"* (ENISA, 2015, s. 60–61).

Podle přílohy IV Nařízení **musejí kvalifikované certifikáty pro autentizaci internetových stránek splňovat následující požadavky**:

- Kvalifikovaný certifikát pro autentizaci internetových stránek musí obsahovat označení, že se certifikát vydává jako kvalifikovaný certifikát pro autentizaci internetových stránek. Nařízení požaduje, aby toto označení bylo alespoň ve formě vhodné pro automatické zpracování. Podle technické normy ETSI EN 319 412-5 V2.2.1 (2016-02) je toto realizováno zápisem do rozšiřující položky certifikátu s názvem QCS *(Qualified Certificate Statement)*, kde jsou umisťovány různé technické údaje včetně statusu kvalifikovaného certifikátu.
- Kvalifikovaný certifikát pro autentizaci internetových stránek musí také obsahovat soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb vytvářejících důvěru, který vydává kvalifikované certifikáty, včetně alespoň členského státu, v němž je poskytovatel usazen. Je-li tímto poskytovatelem právnická osoba, musí obsahovat její název a případné registrační číslo uvedené v úředních záznamech, což v případě ČR znamená např. IČO. Je-li tímto poskytovatelem fyzická osoba, musí obsahovat její jméno.
- Kvalifikovaný certifikát pro autentizaci internetových stránek musí již z definice obsahovat identifikaci fyzické nebo právnické osoby, jíž byl vydán. Jde-li o fyzickou osobu, tak tato identifikace musí zahrnovat alespoň jméno osoby, nebo pseudonym, přičemž použití pseudonymu musí být jasně vyznačeno [srov. požadavek přílohy I písm. c) pro kvalifikované certifikáty pro elektronické podpisy]. Jde-li o právnickou osobu, tak tato identifikace musí zahrnovat alespoň název právnické osoby a případné registrační číslo uvedené v úředních záznamech [srov. požadavek přílohy II písm. c) Nařízení pro kvalifikované certifikáty pro elektronické pečetě].
- Na rozdíl od kvalifikovaných certifikátů pro elektronický podpis nebo elektronickou pečeť se však pro kvalifikovaný certifikát pro autentizaci internetových stránek vyžadují ještě další údaje specifikující subjekt, jemuž byl certifikát vydán. Jedná se o vybrané údaje z adresy (včetně alespoň města a státu) dané fyzické nebo právnické osoby, jak je uvedena v případných úředních záznamech.
- Dalším nezbytným údajem uvedeným v kvalifikovaném certifikátu pro autentizaci internetových stránek je název domény nebo domén, které provozuje fyzická nebo právnická osoba, jíž je certifikát vydán. Podle stanoviska odboru eGovernmentu Ministerstva vnitra dostupného z: <https://www.mvcr.cz/clanek/stanovisko-k-pouziti-kvalifikovanych-certifikatu-pro-autentizaci-internetovych-stranek.aspx> v případě, kdy žadatel o certifikát není schopen kvalifikovanému poskytovateli doložit, že provozuje příslušnou doménu, příp. domény, nebo kvalifikovaný poskytovatel služeb vytvářejících důvěru nemůže tuto skutečnost ověřit, pak nelze kvalifikovaný certifikát pro autentizaci internetových stránek tomuto žadateli vydat (Ministerstvo vnitra, 2018, s. 3).

– Kvalifikovaný certifikát pro autentizaci internetových stránek (jako každý kvalifikovaný certifikát) musí obsahovat označení začátku a konce doby platnosti certifikátu. Jde o nejdelší platnost, jakou kvalifikovaný certifikát může mít, přičemž za určitých podmínek může být tato platnost zkrácena, avšak informace o předčasném zneplatnění certifikátu nemůže být jeho součástí, ale poskytuje ji podle článku 24 odst. 4 Nařízení spoléhající se straně každý kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty, a to automatizovaným způsobem, který je spolehlivý, bezplatný a účinný, a k tomu kdykoli i po skončení doby platnosti certifikátu ve smyslu právě té platnosti, která je v certifikátu vyznačena dle citované přílohy IV písm. f).
– Kvalifikovaný certifikát pro autentizaci internetových stránek (jako každý kvalifikovaný certifikát) musí také obsahovat identifikační číslo certifikátu, které je jedinečné pro daného kvalifikovaného poskytovatele služeb vytvářejících důvěru. Podle tohoto čísla lze také certifikát případně identifikovat v seznamu předčasně zneplatněných certifikátů, popř. v evidenci vydaných certifikátů, kterou vede podle článku 24 odst. 2 písm. k) Nařízení každý kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty.
– Důvěryhodnost kvalifikovaného certifikátu pro autentizaci internetových stránek je zaručena jeho opatřením zaručeným elektronickým podpisem nebo zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává. Vytváří se tím takzvaný řetěz důvěry, v němž se důvěryhodnost kvalifikovaného certifikátu pro autentizaci internetových stránek zaručuje důvěryhodností certifikátu (nebo dalšího řetězu certifikátů) kvalifikovaného poskytovatele služeb vytvářejících důvěru.
– Pro ověření zmíněného řetězu důvěry je třeba mít možnost použít všechny certifikáty z celého řetězu. Proto součástí kvalifikovaného certifikátu pro autentizaci internetových stránek musí být údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť poskytovatele služeb vytvářejících důvěru podle předchozího odstavce.
– Nezbytnou součástí ověřovacího procesu certifikátu je ověření, zda nebyl certifikát předčasně zneplatněn. Proto součástí kvalifikovaného certifikátu pro autentizaci internetových stránek musí být také údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu.

Na rozdíl od článku 28 odst. 4 a čl. 38 odst. 4 Nařízení, které upřesňují pravidlo, že zneplatněný kvalifikovaný certifikát pro elektronický popis, resp. zneplatněný kvalifikovaný certifikát pro elektronickou pečeť, ztrácí okamžikem zneplatnění platnost a jeho status se nemůže v žádném případě změnit zpět, není toto pravidlo pro kvalifikovaný certifikát pro autentizaci internetových stránek takto explicitně v Nařízení vyjádřeno, avšak v praxi je plně dodržováno i v tomto případě. Obdobně není pro kvalifikovaný certifikát pro autentizaci internetových stránek řešen postup dočasného pozastavení platnosti. Nicméně i na tyto kvalifikované certifikáty se plně vztahuje článek 24 odst. 3, který říká, že jestliže se kvalifikovaný poskytovatel služeb vytvářejících důvěru vydávající kvalifikované certifikáty rozhodne určitý certifikát zneplatnit, ať již na základě vlastního podnětu, nebo na základě žádosti, zaeviduje toto zneplatnění ve své databázi certifikátů a zveřejní jej, přičemž zneplatnění nabývá účinku okamžitě po zveřejnění. V případě zneplatnění na žádost takto musí učinit nejpozději do 24 hodin od obdržení žádosti. Pro kvalifikované poskytovatele

kvalifikovaných certifikátů pro autentizaci internetových stránek usazené v ČR dále platí, že pokyn pro zneplatnění tohoto certifikátu jim může dát na základě § 13 odst. 2 zák. č. 297/2016 Sb. také Digitální a informační agentura, resp. do 31. března 2023 mohlo také dát Ministerstvo vnitra, a to v případě, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán, nebo pokud byl vydán na základě nepravdivých údajů.

Související ustanovení:
čl. 3 odst. 38, 39 – Definice, čl. 24 – Požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru, čl. 28 odst. 4 – Kvalifikované certifikáty pro elektronické podpisy, čl. 38 odst. 4 – Kvalifikované certifikáty pro elektronické pečetě

Související předpisy:
§ 13 zák. o právu na digitální služby

Literatura:
DONÁT, J., MAISNER, M., PIFFL, R. *Nařízení eDIAS*. Komentář. 1. vyd. Praha: C. H. Beck, 2017.

ENISA. *Analysis of standards related to Trust Service Providers Mapping of requirements of eIDAS to existing standards* [online]. Heraklion, Greece: ENISA, 2015. Citace 1. 11. 2020. Dostupné z: <https://www.enisa.europa.eu/publications/tsp_standards_2015>.

ENISA. *Security guidelines on the appropriate use of qualified electronic seals* [online]. Heraklion, Greece: ENISA, 2017. Citace 1. 11. 2020. Dostupné z: <https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-seals>.

EVROPSKÁ KOMISE. *Trusted List Browser: Tool to browse the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL)* [online]. Citace 1. 10. 2020. Dostupné z: <https://webgate.ec.europa.eu/tl-browser/#/>.

EVROPSKÁ KOMISE. *Informace o důvěryhodných seznamech členských států ve strojově čitelné podobě zveřejněné podle článku 22 odst. 3 Nařízení.* [online]. Citace 1. 10. 2020. Dostupné z: <http://uri.etsi.org/19612/TSLTag>.

EVROPSKÁ KOMISE. *Seznam certifikovaných kvalifikovaných prostředků pro vytváření elektronických podpisů a certifikovaných kvalifikovaných prostředků pro vytváření elektronických pečetí* [online]. Citace 1. 12. 2020. Dostupné z: <https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD>. (Aktuální seznam k uvedenému datu ve formátu PDF je dostupný tamtéž).

KMENT, V. *Elektronické právní jednání*. Praha: Wolters Kluwer, 2018.

LECHNER, T., MITWALLYOVÁ, H. Legal Analysis of the Development of Data Mailboxes in the Context of the eIDAS Regulation. In VAŇKOVÁ, I. (ed.) *Proceedings of the 12th International Scientific Conference*, Public Economics and Administration 2017. Ostrava: VŠB – Technical University of Ostrava, 2017.

MATES, P. (ed.) at al. *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges, 2019.

MINISTERSTVO VNITRA. *Dokument konkretizující požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru a jimi poskytované kvalifikované služby vytvářející důvěru [DKP]* [online]. Praha: MV, 2018. Citace 1. 10. 2020. Dostupné z: <https://www.mvcr.cz/soubor/dkpv2-pdf.aspx>.

MINISTERSTVO VNITRA. *Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru* [online]. Citace 1. 12. 2022. Dostupné z: <https://www.mvcr.cz/vyzkum/docDetail.aspx?docid=22022190&docType=ART>.

MINISTERSTVO VNITRA. *Seznam certifikátů, na jejichž základě kvalifikovaní poskytovatelé služeb vytvářejících důvěru podepisují zaručeným elektronickým podpisem nebo pečetí zaručenou el. pečetí vydané kvalifikované certifikáty nebo vydaná kvalifikovaná el. časová razítka* [online]. Citace 1. 10. 2020. Dostupné z: <https://www.mvcr.cz/clanek/seznam-certifikatu-na-jejichz-zak