



Univerzita Komenského v Bratislave  
Právnická fakulta

Šafárikovo nám. 6  
P. O. BOX 313  
810 00 Bratislava

APVV-17-0403 Vplyv vzájomného  
uznávania prostriedkov  
elektronickej identifikácie na  
elektronické služby verejnej správy

# ZDOKONALENÝ ELEKTRONICKÝ PODPIS AKO UZNANÝ SPÔSOB AUTORIZÁCIE A JEHO ÚČINKY ROVNOCENÉ S VLASTNORUČNÝM PODPISOM

APVV-17-0403 Vplyv vzájomného uznávania prostriedkov elektronickej identifikácie na  
elektronické služby verejnej správy

**Vypracoval:**

JUDr. Jozef Andraško, PhD.

**Odberateľ:**

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI)

**Kontaktná osoba:**

JUDr. Monika Mušutová





**Právna analýza je výstupom z projektu APVV-17-0403 Vplyv vzájomného uznávania prostriedkov elektronickej identifikácie na elektronické služby verejnej správy.**

**Právna analýza vychádza z právneho stavu k 30.12.2021 a jej zameranie bolo špecifikované a konzultované s odberateľom prostredníctvom mailovej komunikácie a online stretnutia.**



## MANAŽÉRSKE ZHRNUTIE

**Otázka č. 1:** *Môže mať na národnej úrovni zdokonalený elektronický podpis v zmysle Nariadenia eIDAS rovnocenné účinky s vlastnoručným podpisom?*

**Odpoveď:** Nariadenie eIDAS nezakazuje, aby elektronické podpisy, ktoré nespĺňajú požiadavky na kvalifikované elektronické podpisy nemali právne účinky rovnocenné s vlastnoručným podpisom na národnej úrovni. Avšak takýto právny účinok elektronických podpisov by musel byť výslovne upravený v právnom poriadku členského štátu. Ponecháva sa na vnútroštátne právo, aby vymedzilo právny účinok elektronických podpisov s výnimkou požiadavky stanovenej v Nariadení eIDAS, podľa ktorej má kvalifikovaný elektronický podpis právny účinok rovnocenný s vlastnoručným podpisom.

**Otázka č. 2:** *Existuje v právnom poriadku Českej republiky právna úprava používania elektronického podpisu, ktorá priznáva aj iným druhom elektronického podpisu ako je kvalifikovaný elektronický podpis rovnocenné právne účinky s vlastnoručným podpisom?*

**Odpoveď:** Právna úprava používania elektronického podpisu v Českej republike je príkladom toho, že na národnej úrovni sú priznané rovnocenné účinky s vlastnoručným podpisom aj iným druhom elektronického podpisu ako je kvalifikovaný elektronický podpis. ZSVD priznáva vo vzťahu k verejnému sektoru nad rámec Nariadenia eIDAS právne účinky vlastnoručného podpisu aj zaručenému (zdokonalenému) elektronickému podpisu, ktorý však musí byť založený na kvalifikovanom certifikáte pre elektronický podpis. V rámci súkromnoprávných vzťahov subjektov je ekvivalentom vlastnoručného podpisu aj obyčajný elektronický podpis.

**Otázka č. 3:** *Možno ustanoviť zdokonalený elektronický podpis za uznaný spôsob autorizácie v zmysle ZoEG? Čo by malo byť obsahom všeobecne záväzného právneho predpisu (vyhlášky), ktorý bude upravovať uznaný spôsob autorizácie?*

**Odpoveď:** Zdokonalený elektronický podpis, ktorý spĺňa požiadavky v zmysle Nariadenia eIDAS môže byť ustanovený za uznaný spôsob autorizácie v zmysle ZoEG. Takýto zdokonalený elektronický podpis by mal byť podobne ako v prípade právnej úpravy Českej republiky založený na kvalifikovanom certifikáte pre elektronický podpis, čím sa zaistí jednoznačné spojenie elektronického podpisu s podpisujúcou osobou.



Zdokonalený elektronický podpis, ktorý je založený na kvalifikovanom certifikáte pre elektronický podpis spĺňa aj zákonné požiadavky, ktoré sú kladené na uznaný spôsob autorizácie v zmysle ZoEG. Vyhláška upravujúca zdokonalený elektronický podpis ako uznaný spôsob autorizácie, ktorú má prijať MIRRI, by mala vyslovene určiť, že uznaným spôsobom autorizácie v zmysle § 23 ods. 1 písm. a) bodu 3 ZoEG je zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis. V predmetnej vyhláške by prostredníctvom odkazov bolo uvedené, že zdokonalený elektronický podpis, ako aj kvalifikovaný certifikát pre elektronický podpis musia spĺňať požiadavky podľa Nariadenia eIDAS.

**Otázka č. 4:** *Aké dopady má akceptovanie zdokonalených elektronických podpisov založených na kvalifikovanom certifikáte pre elektronický podpis z hľadiska povinností vyplývajúcich z čl. 2 Vykonávacieho rozhodnutia 2015/1506 (v nadväznosti na čl. 27 Nariadenia eIDAS)?*

**Odpoveď:** Členské štáty nie sú automaticky povinné uznávať iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 Vykonávacieho rozhodnutia 2015/1506. Táto povinnosť vznikne členským štátom len vtedy ak členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkne iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie. Možnosti validácie podpisu musia spĺňať konkrétne požiadavky v zmysle čl. 2 ods. 2 Vykonávacieho rozhodnutia 2015/1506 a členské štáty by mali prijímajúcim členským štátom poskytnúť ľahko dostupné informácie týkajúce sa týchto validačných nástrojov.



## 1. Otázky a ich kontext

Právna úprava elektronického podpisu a iných elektronických nástrojov na úrovni Európskej únie (ďalej len „EÚ“) je imanentnou súčasťou poskytovania elektronických služieb verejnej správy. V rámci poskytovania služieb verejnej správy sa v mnohých prípadoch vyžaduje podpísanie elektronického dokumentu. Predmetom regulácie nariadenia EP a Rady 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (ďalej len „Nariadenie eIDAS“) je okrem iného aj právna úprava existencie, požiadaviek, vytvárania a uznávania elektronických podpisov a ich právnych účinkov.

V rámci diskusií s odberateľom a ohľadom na aplikačné problémy v praxi sme identifikovali viacero otázok, ktoré je potrebné z pohľadu elektronického podpisu riešiť.

V prvom rade, Nariadenie eIDAS priznáva rovnocenné právne účinky s vlastnoručným podpisom len najvyššej úrovni elektronického podpisu, ktorým je kvalifikovaný elektronický podpis.<sup>1</sup> Avšak pre podpisujúce osoby môže byť finančne náročné zabezpečiť kvalifikované zariadenie na vyhotovenie elektronického podpisu (napr. čipová karta, USB token), ktoré je pre vytvorenie kvalifikovaného elektronického podpisu nevyhnutné.<sup>2</sup> Taktiež môže nastať situácia, kedy certifikátu pre kvalifikované zariadenie na vyhotovovaní podpisu skončí platnosť, a teda už nebude spĺňať požiadavky pre kvalifikovaný elektronický podpis ale aspoň pre zdokonalený elektronický podpis. Preto je otázne, či môžu mať aj nižšie úrovne elektronického podpisu ako je kvalifikovaný elektronický podpis rovnocenné právne účinky s vlastnoručným podpisom na národnej úrovni. V tejto súvislosti sa v rámci prvej otázky analýza zameria na odpoveď, či:

„Môže mať na národnej úrovni zdokonalený elektronický podpis v zmysle Nariadenia eIDAS rovnocenné účinky s vlastnoručným podpisom?“ (**Otázka č. 1**)

V druhom rade, je potrebné sa zamerať aj na iné členské štáty a ich právne poriadky, ktoré upravujú problematiku využívania konkrétnych druhov elektronických podpisov pri

<sup>1</sup> Čl. 25 ods. 2 Nariadenia eIDAS.

<sup>2</sup> Čl. 3 bod 12 Nariadenia eIDAS.



komunikácii s verejnou správou. Z tohto dôvodu sme si vybrali právny poriadok Českej republiky, ktorý obsahuje právnu úpravu používania konkrétnych druhov elektronického podpisu v rámci právnych konaní s orgánmi verejnej moci ale aj na úrovni súkromnoprávných vzťahov. Z tohto dôvodu sa zameriame na nasledovnú otázku:

*„Existuje v právnom poriadku Českej republiky právna úprava používania elektronického podpisu, ktorá priznáva aj iným druhom elektronického podpisu ako je kvalifikovaný elektronický podpis rovnocenné právne účinky s vlastnoručným podpisom?“ (Otázka č. 2)*

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) (ďalej len „ZoEG“) upravuje niekoľko spôsobov ako osoby iné ako orgány verejnej moci vykonávajú autorizáciu elektronického podania ak sa podľa zákona podáva v elektronickej podobe a zákon neustanovuje iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitou podania vlastnoručný podpis.<sup>3</sup> ZoEG v takýchto prípadoch neuvádza ako možnosť vykonania autorizácie elektronického podania zdokonaleným elektronickým podpisom. Avšak, jedným z týchto spôsobov je vykonanie autorizácie elektronického podania uznaným spôsobom autorizácie.<sup>4</sup> Z tohto dôvodu sa zameriame na nasledovnú otázku:

*Možno ustanoviť zdokonalený elektronický podpis za uznaný spôsob autorizácie v zmysle ZoEG? Čo by malo byť obsahom všeobecne záväzného právneho predpisu (vyhlášky), ktorý bude upravovať uznaný spôsob autorizácie? (Otázka č. 3)*

Nariadenie eIDAS osobitne upravuje v čl. 27 vo vzťahu k verejnému sektoru používanie konkrétnych druhov elektronických podpisov a ich uznávanie. V prípade ak by sa za uznaný spôsob autorizácie ustanovil zdokonalený elektronický podpis, ktorý je založený na kvalifikovanom certifikáte pre elektronický podpis, bude potrebné zodpovedať na nasledujúcu otázku:

---

<sup>3</sup> § 23 ods. 1 písm. a) ZoEG.

<sup>4</sup> § 23 ods. 1 písm. a) bod 3 ZoEG.



*Aké dopady má akceptovanie zdokonalených elektronických podpisov založených na kvalifikovanom certifikáte pre elektronický podpis z hľadiska povinností vyplývajúcich z čl. 2 Vykonávacieho rozhodnutia Komisie EÚ 2015/1506 (v nadväznosti na čl. 27 Nariadenia eIDAS)?*

Pri vypracovaní predkladanej analýzy postupujeme takým spôsobom, že uvedieme právny stav *de lege lata*, ktorý následne zasadíme do slovenských reálií a predloženej otázky. Po jej zodpovedaní v prípade identifikovania nedostatkov odporučíme ideálny postup.

## **2 Analýza právneho stavu**

V rámci tejto časti analýzy budeme diskutovať aktuálny právny stav s ohľadom na obsahové zameranie jednotlivých otázok. Postupovať budeme podľa položených otázok odberateľom.

### **2.1 Otázka č. 1 (Právne účinky zdokonaleného elektronického podpisu rovnocenné s vlastnoručným podpisom)**

Z komunikácie s odberateľom projektu vystala požiadavka analyzovať či môže mať na národnej úrovni zdokonalený elektronický podpis v zmysle Nariadenia eIDAS rovnocenné účinky s vlastnoručným podpisom. V tejto súvislosti najskôr dôjde k ozrejmieniu elektronického podpisu z teoreticko-technického hľadiska a následne upriamime našu pozornosť na právnu úpravu elektronického podpisu a jeho právnych účinkov v zmysle Nariadenia eIDAS.

#### **2.1.1 Teoreticko-právne východisko a bezpečnostné požiadavky na vlastnoručný podpis**

Vo fyzickom svete vytvára fyzická osoba vlastnoručný podpis, čím prejavuje svoju vôľu a vyjadruje súhlas s obsahom podpísaného dokumentu.

Písomnú formu právneho úkonu tvoria dve pojmové náležitosti. Prvou je písomnosť, ktorá spočíva v tom, že obsah prejavu vôle je zachytený v texte listiny. Druhou pojmovou náležitosťou je podpis konajúcej osoby. Podpisom sa završuje písomný právny úkon, a tým



vyvoláva zamýšľané právne následky. Podpis danej osoby sa musí javiť ako podpis konkrétnej osoby, nakoľko je potrebné z podpisu identifikovať podpisujúceho. V zmysle § 40 ods. 4 zákona č. 40/1964 Zb. Občianskeho zákonníka je písomná forma zachovaná, ak je právny úkon urobený telegraficky, ďalekopisom alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon urobila. Písomná forma je zachovaná vždy, ak právny úkon urobený elektronickými prostriedkami je podpísaný kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečatou.

Z bezpečnostného hľadiska plní vlastnoručný podpis nasledujúce bezpečnostné požiadavky:

- **identifikuje osobu, ktorá dokument podpísala,**
- **zaručuje autentickosť (originalitu) dokumentu, aby nedošlo k modifikácii dokumentu po podpise,**
- **vyjadruje súhlas podpisovateľa s obsahom dokumentu,**
- **nemožno ho preniesť na iný dokument,**
- **je nesfalšovateľný, nakoľko vytvoriť ho vie len podpisovateľ a overiť ho dokáže každý.<sup>5</sup>**

Ako však zabezpečiť, aby vyššie uvedené bezpečnostné požiadavky vlastnoručného podpisu boli naplnené aj vo virtuálnom priestore v situáciách, kedy sa vyžaduje podpísanie elektronického dokumentu? Odpoveď na túto otázku nám dáva **elektronický podpis**.

Elektronický podpis má viacero foriem. V praxi sa môžeme stretnúť s napísaním mena do elektronického dokumentu, naskenovaním vlastnoručného podpisu a jeho vložením do elektronického dokumentu, zadaním PIN kódu, kliknutím tzv. „click-wrap“, elektronickým podpisom vytvoreným na podpisový tablet alebo s digitálnym podpisom, ktorý je založený na kryptografii verejného kľúča.

Nie všetky druhy vyššie uvedených elektronických podpisov spĺňajú bezpečnostné požiadavky, ktoré sa kladú na vlastnoručný podpis. Pri napísaní mena do elektronického dokumentu alebo naskenovaní vlastnoručného podpisu a vložením ho do elektronického

---

<sup>5</sup> OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015. s. 108. [online] [cit. 10.9.2020]. Dostupné na: <<https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-8gf.html>>.





dokumentu sa môže stať, že takéto elektronické podpisy budú vkladané aj na iné dokumenty, nebudú vyjadrovať súhlas podpisovateľa s obsahom dokumentu a nebudú zaručovať originalitu dokumentu. Pri rôznych úkonoch, a to najmä v súkromnom sektore, napríklad v bankách alebo u mobilných operátorov osoba podpisuje rôzne elektronické dokumenty prostredníctvom podpisových tabletov. Avšak osoba si nikdy nemôže byť istá, že v danom momente nepodpisuje aj iný dokument.

### 2.1.2 Právne východiská pre elektronický podpis

Problematiku elektronických podpisov a ich právnych účinkov upravuje **Nariadenie eIDAS**.<sup>6</sup> Niektoré otázky, ktoré sa nevyriešili v legislatívnom procese EÚ boli ponechané na právnu úpravu jednotlivých členských štátov EÚ. Tie čiastočne reflektuje slovenský zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov.

Nariadenie eIDAS definuje **tri druhy elektronických podpisov** podľa úrovne bezpečnosti<sup>7</sup>, konkrétne:

1. **obyčajný elektronický podpis**
2. **zdokonalený elektronický podpis**
3. **kvalifikovaný elektronický podpis**

#### Ad 1)

Najnižšiu úroveň predstavuje tzv. **obyčajný elektronický podpis**, ktorý je definovaný ako: „*údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie.*“<sup>8</sup> Za obyčajný elektronický podpis možno považovať v zásade čokoľvek, čo vieme zdigitalizovať (napr. heslo, PIN, obrázok a pod.) a pripojiť k iným údajom (podpisovanému dokumentu).<sup>9</sup>

<sup>6</sup> Nariadenie eIDAS upravuje taktiež problematiku elektronických pečatí a iných elektronických nástrojov. Analýza týchto inštitútov nie je predmetom predkladaného stanoviska.

<sup>7</sup> Resp. záruk, ktoré dané riešenie elektronického podpisu poskytuje.

<sup>8</sup> Čl. 3 bod 10 Nariadenia eIDAS.

<sup>9</sup> Za obyčajný elektronický podpis by sme mohli považovať aj (zdigitalizovaný) hlas. Bližšie pozri: SMEJKAL, V. a KODL, J. a UŘIČAŘ, M.: *Elektronický podpis podle nařízení eIDAS*. In *Revue pro právo a technologie*, 2015, č. 11, s. 218-219, 228.



V súvislosti s vytvorením elektronického podpisu platí, že údaje pre vytváranie elektronického podpisu predstavujú: „jedinečné údaje, ktoré podpisujúca osoba používa na vytvorenie elektronického podpisu.“<sup>10</sup> Pri použití asymetrického šifrovania môžeme za takéto údaje považovať súkromný kľúč.

#### Ad 2)

Vyššiu úroveň bezpečnosti predstavuje **zdokonalený elektronický podpis**.<sup>11</sup> V zmysle Nariadenia eIDAS ide o elektronický podpis, ktorý spĺňa požiadavky podľa článku 26 Nariadenia eIDAS. Prvou požiadavkou je **jedinečnosť spojenia zdokonaleného elektronického podpisu s fyzickou osobou, ktorá vyhotovuje elektronický podpis**, čiže podpisovateľom.<sup>12</sup> Ďalšou požiadavkou na zdokonalený elektronický podpis je **určenie totožnosti podpisovateľa**. Zdokonalený elektronický podpis musí taktiež spĺňať požiadavku, aby bol **vyhotovený pomocou údajov na vyhotovenie elektronického podpisu**, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou (napr. súkromný kľúč). Poslednou požiadavkou je, aby zdokonalený elektronický podpis bol **prepojený s údajmi, ktoré sa ním podpisujú**, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.<sup>13</sup>

#### Ad 3)

Najvyššiu úroveň bezpečnosti predstavuje **kvalifikovaný elektronický podpis**. Tak ako v prípade zdokonaleného elektronického podpisu aj kvalifikovaný elektronický podpis je jedinečne spojený s podpisovateľom. Popri požiadavkách, ktoré musí spĺňať zdokonalený elektronický podpis, musí byť kvalifikovaný elektronický podpis navyše **vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu** (napr.

<sup>10</sup> Čl. 3 bod 13 Nariadenia eIDAS.

<sup>11</sup> Špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov sú upravené vo vykonávacom rozhodnutí Komisie (EÚ) 2015/1506 z 8. septembra 2015, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu.

<sup>12</sup> Čl. 3 bod 9 Nariadenia eIDAS.

<sup>13</sup> Tieto požiadavky sú typické pre elektronické podpisy, ktoré sú všeobecne známe pod názvom digitálne podpisy.



čipová karta, USB token) a musí byť **založený na kvalifikovanom certifikáte pre elektronické podpisy**<sup>14</sup>, ktorý vydáva kvalifikovaný poskytovateľ služieb dôvery.<sup>15</sup>

### 2.1.3 Právne účinky elektronického podpisu

Elektronickému podpisu **nesmú byť odopierané právne účinky** a nesmie byť odmietaný ako **dôkaz v súdnom konaní** iba z toho dôvodu, že **má elektronickú podobu**, alebo **že nespĺňa požiadavky na kvalifikované elektronické podpisy**. V tomto prípade ide o uplatnenie princípu nediskriminácie, ktorý znamená, že ani obyčajnému a zdokonalenému elektronickému podpisu nesmú byť odopierané právne účinky a nesmú byť odmietané ako dôkaz v súdnom konaní len z dôvodu, že nespĺňajú požiadavky na kvalifikovaný elektronický podpis. Ponecháva sa však na vnútroštátne právo, aby vymedzilo právny účinok elektronických podpisov s výnimkou požiadavky stanovenej v Nariadení eIDAS, podľa ktorej má **kvalifikovaný elektronický podpis právny účinok rovnocenný s vlastnoručným podpisom, a to v celej EÚ**.<sup>16</sup>

Inými slovami, **nie je vylúčené, aby elektronické podpisy, ktoré nespĺňajú požiadavky na kvalifikované elektronické podpisy, nemohli mať právne účinky rovnocenné s vlastnoručným podpisom** na národnej úrovni. Avšak takýto právny účinok elektronických podpisov by musel byť výslovne upravený v právnom poriadku členského štátu.

<sup>14</sup> Požiadavky na kvalifikované certifikáty pre elektronické podpisy sú uvedené v prílohe II Nariadenia eIDAS.

<sup>15</sup> Čl. 3 bod 12 Nariadenia eIDAS.

<sup>16</sup> Recitál 49 a čl. 25 Nariadenia eIDAS.



## 2.2 Otázka č. 2 (Právna úprava elektronického podpisu v právnom poriadku Českej republiky)

V rámci druhej otázky preskúmame právnu úpravu používania elektronického podpisu v Českej republike. Zameriame sa na možnosti používania rôznych druhov elektronického podpisu pri komunikácii s verejnou správou a ich právne účinky rovnocenné s vlastnoručným podpisom.

### 2.2.1 Analýza používania elektronického podpisu v ZSVD

Problematika podpisovania elektronickým podpisom je v právnom poriadku Českej republiky upravená zákonom č. 297/2016 Sb. o službách vytvárajúcich dôveru pro elektronické transakce (ďalej len „ZSVD“).<sup>17</sup>

Ustanovenia § 5 až § 7 ZSVD predstavujú všeobecnú právnu úpravu **podpisovania elektronických dokumentov**<sup>18</sup> konkrétnym druhom elektronického podpisu v závislosti od typu subjektu, ktorý podpisuje elektronický dokument a úkonu, ktorý vykonáva v rámci danej pôsobnosti.

ZSVD predstavuje vykonávací zákon k Nariadeniu eIDAS, a teda neupravuje právny rámec pre existenciu, požiadavky, vytváranie a uznanie elektronických podpisov a elektronických pečatí ale upravuje najmä, v akých prípadoch sa má používať konkrétny typ elektronického podpisu a elektronickej pečate.<sup>19</sup>

V závislosti od subjektu, ktorý podpisuje elektronické dokumenty, resp. od povahy úkonu alebo právneho konania ZSVD upravuje:

1. kvalifikovaný elektronický podpis (§ 5 ZSVD),
2. uznaný elektronický podpis (§ 6 ZSVD),
3. iný typ elektronického podpisu (§ 7 ZSVD),

<sup>17</sup> Dostupné na: <https://www.zakonyprolidi.cz/cs/2016-297>.

<sup>18</sup> ZSVD nedefinuje pojem elektronický dokument. Tento pojem je definovaný v čl. 3 bod. 35 Nariadenia eIDAS. Elektronický dokument predstavuje akýkoľvek obsah, ktorý je uložený v elektronickej forme. Nariadenie eIDAS uvádza ako príklady text alebo zvukový, obrazový či audiovizuálny záznam.

<sup>19</sup> Pozri VACULÍK, L.: Obecné dopady nařízení eIDAS do činnosti soudních exekutorů. Komorní listy 3/2018, s. 32. Dostupné na: <https://www.ekcr.cz/admin/priloha//2018-03-Komorni-listy.pdf>.



## Ad 1)

### § 5 Kvalifikovaný elektronický podpis

*K podepisování elektronickým podpisem lze použít pouze kvalifikovaný elektronický podpis, podepisuje-li elektronický dokument, kterým*

*a) činí úkon nebo právně jedná stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem nebo jejich orgán anebo jiná jejich součást (dále jen „veřejnoprávní podepisující“), nebo*

*b) činí úkon osoba neuvedená v písmenu a) při výkonu své působnosti.*

**Kvalifikovaný elektronický podpis** predstavuje najvyššiu úroveň elektronického podpisu, ktorý musí spĺňať požiadavky pre tento druh elektronického podpisu v zmysle Nariadenia eIDAS.

Subjekty, ktoré sú zvedené v § 5 ZSVD sú povinné podpisovať elektronické dokumenty výlučne kvalifikovaným elektronickým podpisom. Túto formu elektronického podpisu musia používať uvedené orgány verejnej moci, ktoré sú v ZSVD označené ako verejnoprávni podpisujúci (písm. a)) a iné fyzické a právnické osoby pri výkone pôsobnosti v oblasti verejnej správy (písm. b)).

Subjekty uvedené v § 5 písm. b) ZSVD môžu v rámci úkonov, ktoré nespádajú do výkonu ich pôsobnosti použiť na podpisovanie elektronických dokumentov aj iný druh elektronického podpisu.<sup>20</sup>

Ustanovenie § 5 ZSVD **nevyklučuje použitie iných podpisových techník a technológií ako je elektronický podpis**. Ako príklad možno uviesť ustanovenie § 18 ods. 2 zákona č.

<sup>20</sup> Príkladom subjektu podľa § 5 písm. b) ZSVD je súdny exekútor. Súdny exekútor môže právne konať v rámci výkonu svojej zákonnej pôsobnosti, ale aj v súkromnoprávnom postavení ako podnikateľ napr. pri uzatváraní zmluvy za účelom materiálneho a personálneho chodu úradu. Bližšie pozri VACULÍK, L.: Obecné dopady nařízení eIDAS do činnosti soudních exekutorů. Komorní listy 3/2018, s. 34. Dostupné na: <https://www.ekcr.cz/admin/priloha//2018-03-Komorni-listy.pdf>.



300/2008 Sb. Zákon o elektronických úkonech a autorizované konverzi dokumentů, ktoré upravuje tzv. **fikciu podpisu**.

§ 18 Provádění úkonů vůči orgánům veřejné moci prostřednictvím datové schránky

(1) Fyzická osoba, podnikající fyzická osoba a právnická osoba může provádět úkon vůči orgánu veřejné moci, má-li zpřístupněnu svou datovou schránku a umožňuje-li to povaha tohoto úkonu, prostřednictvím datové schránky.

(2) **Úkon učiněný osobou** uvedenou v § 8 odst. 1 až 4 nebo pověřenou osobou, pokud k tomu byla pověřena, **prostřednictvím datové schránky má stejné účinky jako úkon učiněný písemně a podepsaný**, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.

Elektronický dokument podpísaný subjektmi uvedenými v § 5 ZSVD musí byť opatrený kvalifikovanou elektronickou časovou pečiatkou.<sup>21</sup>

**Ad 2)**

§ 6 Uznávaný elektronický podpis

(1) K podepisování elektronickým podpisem lze použít pouze uznávaný elektronický podpis, podepisuje-li se elektronický dokument, kterým se činí úkon vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti.

(2) Uznávaným elektronickým podpisem se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.

<sup>21</sup> § 11 ods. 1 ZVSE. V českém jazyku sa používa pojem „elektronické časové razítko.“



Nižšiu úroveň elektronického podpisu predstavuje **uznávaný elektronický podpis**.

Za uznávané elektronické podpisy sa považujú:

- **zaručený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis,**
- **kvalifikovaný elektronický podpis.**

V ZSVD ako aj českom preklade Nariadenia eIDAS sa nepoužíva pojem zdokonalený elektronický podpis (*advanced electronic signature*) tak ako v slovenskom preklade ale používa sa pojem zaručený elektronický podpis.

Ustanovenie § 6 ZSVD upravuje situácie, kedy (súkromnoprávna) **osoba právne koná voči verejnoprávnym podpisujúcim a ďalším osobám uvedeným v § 5 ZSVD**. V takýchto prípadoch môže podpisujúca osoba použiť **len uznávaný elektronický podpis**. Odosielateľ elektronického dokumentu (napr. účastník konania pri podávaní návrhu) je v podriadenom vzťahu voči subjektom uvedeným v § 5 ZSVD. Ako príklady takýchto dokumentov možno uviesť podania a žiadosti za podmienky, že právny predpis vyžaduje ich podpísanie.<sup>22</sup>

Z vyššie uvedeného vyplýva, že ustanovenie § 6 **priznáva nad rámec Nariadenia eIDAS právne účinky vlastnoručného podpisu aj zaručenému elektronickému podpisu, ktorý je založený na kvalifikovanom certifikáte pre elektronický podpis**.

Základným dôvodom, prečo český zákonodarca rozšíril množinu elektronických podpisov, ktoré majú aspoň vo vzťahu k verejnému sektoru vo vrchnostenskom postavení účinky vlastnoručného podpisu, sú finančné náklady, ktoré by museli subjekty vynaložiť na zabezpečenie kvalifikovaného prostriedku pre vytváranie elektronického podpisu. V dôvodovej správe k návrhu ZSVD sa uvádza, že nie je dôvod takýto druh elektronického podpisu vo vzťahu k verejnej správe zavrhnúť, nakoľko zaručený elektronický podpis je založený na kvalifikovanom certifikáte a disponuje dostatočnou mierou autenticity.<sup>23</sup>

Zaručený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis musí spĺňať požiadavky na tento druh elektronického podpisu v zmysle Nariadenia eIDAS.

<sup>22</sup> Dôvodová správa k návrhu ZSVD, s. 35.

<sup>23</sup> Tamže. V EÚ sú aj iné členské štáty, ktoré priznali rovnocenné účinky s vlastnoručným podpisom aj iným druhom elektronického podpisu ako je kvalifikovaný elektronický podpis. Ako príklad možno uviesť Holandsko a Belgicko. Bližšie pozri: <https://www.signicat.com/blog/how-to-take-an-electronic-signature-to-court-across-europe>.



### Ad 3)

#### § 7 Jiný typ elektronického podpisu

*K podepisování elektronickým podpisem lze použít zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu, podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 .*

Ustanovenie § 7 ZSVD upravuje podpisovanie elektronických dokumentov v rámci právnych konaní iných subjektov, ktoré sú uvedené v § 5 ZSVD, adresované subjektom uvedeným v § 5 ZSVD v inom než vrchnostenskom postavení alebo adresované iným subjektom než uvedeným v § 5 ZSVD.<sup>24</sup>

V takýchto prípadoch možno elektronický dokument podpísať:

- zaručeným elektronickým podpisom,
- zaručený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis
- kvalifikovaný elektronický podpis.
- iný typ elektronického podpisu.

Za iný typ elektronického podpisu možno považovať obyčajný elektronický podpis v zmysle Nariadenia eIDAS.

**Český zákonodarca rozširuje paritu s vlastnoručným podpisom i na tieto typy elektronického podpisu.<sup>25</sup>**

#### 2.2.2 Elektronická pečať

Pre úplnosť sa zameriame aj na **elektronickú pečať**, ktorá sa využíva vo vzťahu k verejnej správe, resp. ho využíva verejná správa. Ustanovenia § 8 až § 10 upravujú problematiku pečatenia elektronického dokumentu. ZSVD podobne ako pri elektronickom podpise aj pri elektronickej pečati definuje niekoľko druhov elektronických pečatí, ktoré možno využiť vo vzťahu k verejnému sektoru a ktoré môže používať verejný sektor.

<sup>24</sup> Tamže, s. 36.

<sup>25</sup> Tamže.





V závislosti od subjektu, ktorý pečatí elektronické dokumenty, resp. od povahy úkonu alebo právneho konania ZSVD upravuje:

- **kvalifikovanú elektronickú pečať** (§ 8 ZSVD)
- **uznávanú elektronickú pečať** (§ 9 ZSVD).
- **iný typ elektronickej pečate** (§ 10 ZSVD).

Verejnoprávny podpisujúci a iná právnická osoba, ak robí úkon pri výkone svojej pôsobnosti, zapečatí dokument v elektronickej podobe kvalifikovanou elektronickou pečaťou za podmienky, ak iný právny predpis neustanovuje ako náležitosť úkonu alebo právneho konania obsiahnutého v dokumente podpis alebo táto náležitosť nevyplýva z povahy úkonu alebo právneho konania.<sup>26</sup>

Verejnoprávny podpisujúci, ktorý zapečatil elektronický dokument opatrí zapečatený elektronický dokument kvalifikovanou elektronickou časovou pečiatkou.<sup>27</sup>

Elektronická pečať ani v najvyššej forme nemá právne účinky rovnocenné s vlastnoručným podpisom. Cieľom kvalifikovanej elektronickej pečate nie je potvrdiť vôľu právnickej osoby ale zabezpečiť integritu (nemennosť) digitálneho predmetu (dokumentu) a potvrdiť jeho pôvod.<sup>28</sup>

Ak sa pečatí elektronický dokument, ktorým sa robí úkon voči verejnoprávnenému podpisujúcemu alebo inej osobe v súvislosti s výkonom ich pôsobnosti, tak sa na pečatenie použije iba uznávaná elektronická pečať. Uznávanou elektronickou pečaťou sa rozumie zaručená elektronická pečať založená na kvalifikovanom certifikáte pre elektronickú pečať alebo kvalifikovaná elektronická pečať.<sup>29</sup>

V prípade iného právneho konania ako uvedeného v § 8 ZSVD sa na pečatenie elektronickou pečaťou môže použiť zaručená elektronická pečať, uznávaná elektronická pečať, prípadne iný typ elektronickej pečate (tzv. obyčajná elektronická pečať).<sup>30</sup>

---

<sup>26</sup> § 8 ZSVD.

<sup>27</sup> § 11 ods. 2 ZSVD.

<sup>28</sup> Ministerstvo vnútra Českej republiky. Metodický pokyn k elektronickým podpisom a pečetím pro veřejnoprávní původce. 2019, s. 11. Dostupné na: <https://www.mvcr.cz/clanek/metodicky-pokyn-k-elektronickym-podpisum-a-pecetim-pro-verejnopravni-puvodce.aspx>

<sup>29</sup> § 9 ZSVD.

<sup>30</sup> § 10 ZSVD.



### 2.3 Otázka č. 3 (Zdokonalený elektronický podpis ako uznaný spôsob autorizácie)

ZoEG upravuje niekoľko spôsobov ako osoby iné ako orgány verejnej moci vykonávajú autorizáciu elektronického podania ak sa podľa zákona podáva v elektronickej podobe a zákon neustanovuje iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitou podania vlastnoručný podpis.<sup>31</sup> Jedným zo spôsobov je vykonanie autorizácie elektronického podania uznaným spôsobom autorizácie.<sup>32</sup>

V prípade, kedy by certifikátu pre kvalifikované zariadenie na vyhotovovaní podpisu (napr. elektronický občiansky preukaz) skončila platnosť, a teda už nebude spĺňať požiadavky pre kvalifikovaný elektronický podpis, je na mieste sa zaoberať otázkou, či by za uznaný spôsob autorizácie mohol byť stanovený zdokonalený elektronický podpis, tak aby mal rovnocenné účinky s vlastnoručným podpisom. Taktiež je na mieste sa zaoberať otázkou, čo by malo byť obsahom všeobecne záväzného právneho predpisu, ktorým MIRRI ustanoví takýto uznaný spôsob autorizácie.

#### 2.3.1 Analýza používania elektronického podpisu v ZoEG

Na národnej úrovni upravuje problematiku používania konkrétnych druhov elektronických podpisov a elektronických pečatí vo vzťahu k verejnej správe ZoEG.

ZoEG umožňuje osobám v rôznych právnych postaveniach, konkrétne orgánu verejnej moci a osobe, ktorá nie je orgánom verejnej moci, použiť rôzne elektronické nástroje na vykonanie autorizácie elektronického podania, resp. elektronického úradného dokumentu.

ZoEG definuje autorizácia úkonu ako vyjadrenie súhlasu s obsahom právneho úkonu a s vykonaním tohto právneho úkonu.<sup>33</sup>

**Orgán verejnej moci** vykonáva autorizáciu elektronického podania alebo elektronického úradného dokumentu:<sup>34</sup>

- a) kvalifikovaným elektronickým podpisom a mandátnym certifikátom s pripojenou kvalifikovanou elektronickou časovou pečiatkou alebo

<sup>31</sup> § 23 ods. 1 písm. a) ZoEG.

<sup>32</sup> § 23 ods. 1 písm. a) bod. 3 ZoEG.

<sup>33</sup> § 3 písm. o) ZoEG

<sup>34</sup> § 23 ods. 1 ZoEG



- b) kvalifikovanou elektronickou pečaťou s pripojenou kvalifikovanou elektronickou časovou pečiatkou.

Praktická situácia, kedy môže dôjsť k autorizácii zo strany orgánu verejnej moci je vyhotovenie elektronického úradného dokumentu, napríklad rozhodnutia, ktoré vydá správny orgán. Ak ZoEG alebo osobitný predpis<sup>35</sup> ustanovuje len povinnosť autorizácie bez označenia konkrétnej osoby alebo osoby v konkrétnom postavení, alebo autorizujúcu osobu označuje len všeobecne ako oprávnenú osobu, orgán verejnej moci na autorizáciu použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu alebo kvalifikovanú elektronickú pečať, ku ktorým sa pripojí kvalifikovaná elektronická časová pečiatka.<sup>36</sup>

Ak ZoEG alebo osobitný predpis (napr. § 222 CSP) vyžaduje autorizáciu konkrétnou osobou alebo osobou v konkrétnom postavení, orgán verejnej moci na autorizáciu použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu, ku ktorému sa pripojí kvalifikovaná elektronická časová pečiatka.<sup>37</sup>

V praxi môže nastať situácia, kedy orgán verejnej moci vydáva elektronický úradný dokument, o ktorom vie, že je určený na použitie do zahraničia, alebo ak o to z dôvodu použitia v zahraničí požiada osoba, ktorej sa takýto dokument vydáva. V takýchto prípadoch orgán verejnej moci na autorizáciu použije kvalifikovaný elektronický podpis vyhotovený s použitím mandátneho certifikátu, ku ktorému sa pripojí kvalifikovaná elektronická pečať a kvalifikovaná elektronická časová pečiatka.<sup>38</sup> Predmetné ustanovenie je výsledkom toho, že v zmysle Nariadenia eIDAS má rovnocenné účinky s vlastnoručným podpisom len kvalifikovaný elektronický podpis a len takýto elektronický podpis bude uznávaný vo všetkých členských štátoch ako vlastnoručný podpis.

**Osoba, ktorá nie je orgánom verejnej moci, vykoná autorizáciu elektronického podania, ak sa podľa ZoEG podáva v elektronickej podobe a zákon neustanovuje iný spôsob autorizácie, alebo, ak je podľa osobitného predpisu náležitou podania vlastnoručný podpis.<sup>39</sup>**

<sup>35</sup> Napríklad ustanovenie § 47 ods. 5 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok).

<sup>36</sup> § 23 ods. 3 ZoEG

<sup>37</sup> § 23 ods. 3 ZoEG

<sup>38</sup> § 23 ods. 3 ZoEG

<sup>39</sup> § 23 ods. 1 písm. a) ZoEG.



1. kvalifikovaným elektronickým podpisom alebo kvalifikovanou elektronickou pečaťou,
2. použitím na to určenej funkcie informačného systému prístupového miesta,
3. uznaným spôsobom autorizácie.

ZoEG pri osobách, ktoré nie sú orgánmi verejnej moci upravuje možnosť autorizovať len elektronické podanie. Elektronickým podaním sú: „údaje vyplnené podľa elektronického formulára, ktoré na účely výkonu verejnej moci elektronicky alebo na účely jeho začatia zasiela orgánu verejnej moci osoba, ktorá je účastníkom konania.“<sup>40</sup> Inými slovami, uvedené elektronické nástroje možno použiť len na autorizáciu elektronických podaní podľa ZoEG, avšak už sa to nevzťahuje na iné právne úkony (napr. verejnoprávna zmluva).

V prípade **použitia na to určenej funkcie** informačného systému prístupového miesta platí, že úroveň záruky musí zodpovedať minimálne úrovni pokročilá v zmysle Nariadenia eIDAS pri splnení podmienok v zmysle § 23 ods. 1 písm. b) ZoEG, teda ak:

- sa zabezpečí uvedenie tejto osoby ako odosielateľa elektronickej správy,
- sa zabezpečí nemennosť obsahu autorizovaného dokumentu do momentu uloženia v elektronickej schránke adresáta,
- sa zabezpečí spojenie autorizovaného dokumentu s identifikátorom osoby odosielateľa a zachovanie väzby medzi nimi,
- to osobitný predpis nezakazuje.

**ZoEG** kladie **pre uznaný spôsob autorizácie** konkrétne zákonné požiadavky. Uznaný spôsob autorizácie musí zabezpečiť:<sup>41</sup>

- spoľahlivú identifikáciu osoby, ktorá autorizáciu vykonala,
- spoľahlivé zachytenie obsahu právneho úkonu, ktorý autorizovala, ako aj
- zhodu medzi autorizovaným právnym úkonom a právnym úkonom, ktorý osoba autorizovala.

Uznaný spôsob autorizácie ustanoví MIRRI všeobecne záväzným právnym predpisom.<sup>42</sup>

<sup>40</sup> § 3 písm. j) ZoEG.

<sup>41</sup> § 23 ods. 2 ZoEG.

<sup>42</sup> § 59 ods. 1 písm. m) ZoEG.



Ak je podľa osobitného predpisu náležitosťou podania **vlastnoručný podpis, ktorý musí byť úradne osvedčený**, vykoná osoba, ktorá nie je orgánom verejnej moci autorizáciu elektronického podania, kvalifikovaným elektronickým podpisom, ktorého kvalifikovaný certifikát obsahuje minimálny súbor osobných identifikačných údajov reprezentujúcich jedinečným spôsobom fyzickú osobu podľa osobitného predpisu<sup>43</sup> a ktorý zahrnul do autorizácie aj kvalifikovanú elektronickú časovú pečať, ktorá určuje dátum a čas, po ktorom nastala autorizácia.<sup>44</sup>

### 2.3.2 Zdokonalený elektronický podpis ako uznaný spôsob autorizácie

Z predchádzajúcej analýzy vyplýva, že aj iným elektronickým podpisom ako je kvalifikovaný elektronický podpis možno priznať rovnocenné účinky s vlastnoručným podpisom. V prípade právneho poriadku Českej republiky sa vo vzťahu k verejnej správe priznávajú právne účinky vlastnoručného podpisu aj zaručenému (zdokonalenému) elektronickému podpisu, ktorý je založený na kvalifikovanom certifikáte pre elektronický podpis.

Vychádzajúc z vyššie uvedeného by bolo možné stanoviť za uznaný spôsob autorizácie v zmysle ZoEG zdokonalený elektronický podpis, ktorý spĺňa požiadavky v zmysle Nariadenia eIDAS. Takýto zdokonalený elektronický podpis by mal byť podobne ako v prípade právnej úpravy Českej republiky založený na kvalifikovanom certifikáte pre elektronický podpis, čím sa zaistí jednoznačné spojenie elektronického podpisu s podpisujúcou osobou.

Využitie zdokonaleného elektronického podpisu založenom na kvalifikovanom certifikáte pre elektronický podpis vo vzťahu k verejnému sektoru dokonca dovoľuje Nariadenie eIDAS, konkrétne v čl. 27 ods. 2.<sup>45</sup>

<sup>43</sup> Bod 1 prílohy vykonávacieho nariadenia Komisie (EÚ) 2015/1501 z 8. septembra 2015 o rámci interoperability podľa článku 12 ods. 8 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Ú. v. EÚ L 235, 9.9.2015) v platnom znení.

<sup>44</sup> § 23 ods. 1 písm. b) ZoEG.

<sup>45</sup> Bližšie pozri 2.4 Otázka č. 4 (Dopady na akceptovanie zdokonaleného elektronického podpisu založenom na kvalifikovanom certifikáte pre elektronický podpis).



ZoEG kladie na uznaný spôsob autorizácie konkrétne zákonné požiadavky, čo znamená, že zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis by musel tieto požiadavky napĺňať.

Vychádzajúc z požiadaviek na zdokonalený elektronický podpis a kvalifikovaný certifikát pre elektronický podpis v zmysle Nariadenia eIDAS možno konštatovať, že tieto zákonné požiadavky by boli splnené. Splnenie požiadaviek uvádzame v tabuľke:

Požiadavky na uznaný spôsob autorizácie (ZoEG)	Požiadavky na zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis (Nariadenie eIDAS)	
Spoľahlivá identifikácia osoby, ktorá autorizáciu vykonala.	Je jedinečne spojený s podpisovateľom.	Kvalifikovaný certifikát pre elektronický podpis zaisťuje jednoznačné spojenie elektronického podpisu s podpisujúcou osobou.
	Umožňuje určenie totožnosti podpisovateľa.	
Spoľahlivé zachytenie obsahu právneho úkonu, ktorý autorizovala.	Je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť.	
Zhoda medzi autorizovaným právnym úkonom a právnym úkonom, ktorý osoba autorizovala.		
	Je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou.	



### 2.3.2.1 Využitie elektronického občianskeho preukazu na podpisovanie po skončení platnosti certifikácie elektronického čipu

Platnosť certifikátu elektronických čipových kariet (*Smart Card Atos CardOS V5.0 QES EAC V1.0 version V1.0.*), ktoré sa používajú aj v prípade elektronických občianskych preukazov skončí 31.12.2022.<sup>46</sup>

Z vyššie uvedenej situácie vyplýva, že od 31.12.2022 elektronický podpis za použitia elektronického občianskeho preukazu (vydaného do 25.6.2021) nebude spĺňať v zmysle Nariadenia eIDAS požiadavky na kvalifikovaný elektronický podpis, nakoľko elektronický občiansky preukaz už nebude považovaný za kvalifikované zariadenie na vyhotovovanie podpisu. Taktiež platí, že 31.12.2022 budú zrušené všetky certifikáty, ktoré elektronický občiansky preukaz obsahuje.<sup>47</sup>

Napriek strate platnosti certifikátu zariadenia na vytváranie elektronického podpisu však bude možné elektronický občiansky preukaz stále považovať za (nekvalifikované) zariadenie na vytváranie iného druhu elektronického podpisu, napr. zdokonaleného elektronického podpisu.

Nevýhodou tohto stavu, a teda že by elektronický podpis vytvorený za použitia elektronického občianskeho preukazu spĺňal požiadavky len na zdokonalený elektronický podpis založeného na kvalifikovanom certifikáte pre elektronický podpis je skutočnosť, že by ho bolo možné používať len na vykonanie autorizácie elektronického podania v zmysle ZoEG ale už nie na iné právne úkony, kde je predpísaná písomná forma. V zmysle § 40 ods. 4 zákona č. 40/1964 Zb. Občianskeho zákonníka je písomná forma zachovaná vždy, ak právny **úkon urobený elektronickými prostriedkami je podpísaný kvalifikovaným elektronickým podpisom** alebo kvalifikovanou elektronickou pečaťou. Nižšia úroveň elektronického podpisu ako kvalifikovaný elektronický podpis by teda túto zákonnú požiadavku nespĺňala.

<sup>46</sup> Dostupné na: [https://www.slovensko.sk/sk/oznamy/detail\\_elektronickym-cipom-na-doteraj](https://www.slovensko.sk/sk/oznamy/detail_elektronickym-cipom-na-doteraj). Ministerstvo vnútra SR od 26.6.2021 vydáva elektronické občianske preukazy, ktoré budú mať implementované nové zariadenie (*CardOS DI V5.4 QES Version 1.0.*). Dostupné na: <https://www.minv.sk/?tlacove-spravy-2&sprava=platnost-certifikatu-pre-vydavanie-e-podpisu-na-obcianskych-preukazoch-a-cudzineckych-dokladoch-konci-26-juna-pouzivat-vydane-certifikaty-vsak-bude-mozne-az-do-konca-roku-2022>

<sup>47</sup> Bližšie pozri: <https://www.nbu.gov.sk/wp-content/uploads/urad/odborne-stanoviska/DS/Ukoncenie-platnosti-certifikacie-QSCD-a-zrusenie-kvalifikovanych-certifikatov-z-dovodu-uvadzania-polozky-QcStatement.pdf>.



### 2.3.3 Vyhláška upravujúca zdokonalený elektronický podpis ako uznaný spôsob autorizácie

Vyhláška upravujúca zdokonalený elektronický podpis ako uznaný spôsob autorizácie, ktorú má prijať MIRRI by mala vyslovene určiť, že uznaným spôsobom autorizácie v zmysle § 23 ods. 1 písm. a) bodu 3 ZoEG je zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre vyhotovenie elektronického podpisu. V predmetnej vyhláške by prostredníctvom odkazov bolo uvedené, že zdokonalený elektronický podpis, ako aj kvalifikovaný certifikát pre elektronické podpisy musia spĺňať požiadavky podľa konkrétnych ustanovení (čl. 26), resp. príloh Nariadenia eIDAS (príloha I).

Ďalšie technické špecifikácie alebo detailnejšie úpravy nie sú potrebné.

V dôvodovej správe k budúcej vyhláške by bolo potrebné zdôvodniť, tak ako vyplýva z vyššie uvedenej analýzy, že aj elektronický podpis nižšej úrovne ako kvalifikovaný elektronický podpis môže mať na národnej úrovni rovnocenné účinky s vlastnoručným podpisom. Taktiež by bolo vhodné uviesť, že požiadavky na zdokonalený elektronický podpis, ktorý je založený na kvalifikovanom certifikáte pre elektronický podpis spĺňa aj elektronický podpis vytvorený za použitia elektronického občianskeho preukazu, ktorého platnosť certifikácie elektronického čipu skončila.

Ak by sa predmetnou vyhláškou stanovil za uznaný spôsob autorizácie zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis, znamenalo by to, že držiteľia elektronických občianskych preukazov, ktorých platnosť certifikácie skončila mohli využívať elektronický občiansky preukaz na autorizáciu elektronického podania, ak sa podľa zákona podáva v elektronickej podobe a zákon neustanovuje iný spôsob autorizácie alebo ak je podľa osobitného predpisu náležitou podania vlastnoručný podpis.





## 2.4 Otázka č. 4 (Dopady na akceptovanie zdokonaleného elektronického podpisu založenom na kvalifikovanom certifikáte pre elektronický podpis)

Nariadenie eIDAS osobitne upravuje v čl. 27 ods. 1 a 2 možnosť používať konkrétne druhy elektronického podpisu vo verejných službách a povinnosť ich uznávania.

### Článok 27 Elektronické podpisy vo verejných službách

1. *Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, vyžaduje zdokonalený elektronický podpis, uznáva tento členský štát zdokonalené elektronické podpisy, zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte pre elektronické podpisy a kvalifikované elektronické podpisy, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.*

2. *Ak členský štát na využívanie služby online, ktorú ponúka subjekt verejného sektora alebo ktorá sa ponúka v jeho mene, **vyžaduje zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, uznáva tento členský štát zdokonalené elektronické podpisy založené na kvalifikovanom certifikáte a kvalifikované elektronické podpisy, a to aspoň tie, ktoré sú vo formátoch alebo ktoré používajú metódy vymedzené vo vykonávacích aktoch uvedených v odseku 5.***

Predmetné ustanovenia predstavujú kompromis medzi jednotlivými členskými štátmi, nakoľko v niektorých členských štátoch sa pri využívaní online verejných službách nevyžadoval kvalifikovaný elektronický podpis ale zdokonalený elektronický podpis (čl. 27 ods. 1), resp. zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis (čl. 27 ods. 2).

Vykonávacím aktom v zmysle čl. 27 ods. 5 Nariadenia eIDAS je vykonávacie rozhodnutie Komisie (EÚ) 2015/1506 z 8. septembra 2015, ktorým sa ustanovujú špecifikácie týkajúce sa formátov zdokonalených elektronických podpisov a zdokonalených



elektronických pečatí, ktoré môžu subjekty verejného sektora uznávať, podľa článkov 27 ods. 5 a 37 ods. 5 Nariadenia eIDAS (ďalej len „**Vykonávacie rozhodnutie 2015/1506**“).

Vykonávacie rozhodnutie 2015/1506 definuje **niekoľko najbežnejších formátov zdokonalených elektronických podpisov**. Členské štáty, ktoré vyžadujú vo vzťahu k online verejným službám zdokonalený elektronický podpis alebo zdokonalený elektronický podpis založený na kvalifikovanom certifikáte, uznajú zdokonalený elektronický podpis XML, CMS alebo PDF na úrovni súladu B, T alebo LT alebo použitie podpisového kontajnera vo formáte ASiC, ak sú tieto podpisy v súlade s technickými špecifikáciami uvedenými v prílohe.<sup>48</sup>

Vykonávacie rozhodnutie 2015/1506 taktiež upravuje situáciu, kedy **možno uznať aj iné formáty elektronických podpisov** než tie, ktoré sú uvedené v článku 1.<sup>49</sup> Členské štáty vyžadujúce zdokonalený elektronický podpis alebo zdokonalený elektronický podpis založený na kvalifikovanom certifikáte vo vzťahu k online verejným službám, uznajú iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 za **splnenia niekoľkých podmienok**. Prvou podmienkou je, aby členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkol iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie.<sup>50</sup>

Ďalšie podmienky sa týkajú splnenia konkrétnych požiadaviek na možnosti validácie, ktoré sú upravené v čl. 2 ods. 2 Vykonávacieho rozhodnutia 2015/1506. Členské štáty by mali prijímajúcim členským štátom poskytnúť ľahko dostupné informácie týkajúce sa týchto validačných nástrojov, čo potvrdzuje aj recitál 7 Vykonávacieho rozhodnutia 2015/1506, v zmysle ktorého: *„ak sa na podpis alebo zapečatenie používajú iné než bežne podporované formáty elektronických podpisov alebo pečatí, je potrebné poskytnúť validačné prostriedky, ktoré umožnia overiť elektronické podpisy alebo pečate cez hranice. S cieľom umožniť, aby sa prijímajúce členské štáty mohli spoľahnúť na uvedené validačné nástroje iného členského štátu, je nevyhnutné poskytnúť ľahko dostupné informácie týkajúce sa týchto validačných nástrojov, a to tým, že sa tieto informácie uvedú v elektronických dokumentoch, v elektronických podpisoch alebo v nosičoch elektronických dokumentov.“*

<sup>48</sup> Čl. 1 Vykonávacieho rozhodnutia 2015/1506.

<sup>49</sup> Medzi iné formáty elektronických podpisov možno zahrnúť napr. JWS. Bližšie pozri: <https://blog.eid.as/>.

<sup>50</sup> Čl. 2 ods. 1 Vykonávacieho rozhodnutia 2015/1506.



Recitál 8 Vykonávacieho rozhodnutia 2015/1506 špecifikuje, že v prípade ak automatizované spracovanie možností validácie pre alternatívne metódy nie je možné, povinnosť uznania v zmysle čl. 27 ods. 1 a 2 Nariadenia eIDAS má byť zachovaná. Inými slovami, možnosti validácie pre alternatívne metódy sa budú vykonávať aj manuálnym spracovaním, ak automatizované spracovanie nie je možné.

Z vyššie uvedeného vyplýva, že členské štáty nie sú automaticky povinné uznávať iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 Vykonávacieho rozhodnutia 2015/1506. Táto povinnosť vznikne členským štátom len vtedy ak členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkne iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie. Možnosti validácie podpisu musia spĺňať konkrétne požiadavky v zmysle čl. 2 ods. 2 Vykonávacieho rozhodnutia 2015/1506 a členské štáty by mali prijímajúcim členským štátom poskytnúť ľahko dostupné informácie týkajúce sa týchto validačných nástrojov.

### **3. Odpovede a navrhované riešenia**

#### **3.1 Otázka č. 1**

Nariadenie eIDAS nezakazuje, aby elektronické podpisy, ktoré nespĺňajú požiadavky na kvalifikované elektronické podpisy nemali právne účinky rovnocenné s vlastnoručným podpisom na národnej úrovni. Avšak takýto právny účinok elektronických podpisov by musel byť výslovne upravený v právnom poriadku členského štátu. Ponecháva sa na vnútroštátne právo, aby vymedzilo právny účinok elektronických podpisov s výnimkou požiadavky stanovenej v Nariadení eIDAS, podľa ktorej má kvalifikovaný elektronický podpis právny účinok rovnocenný s vlastnoručným podpisom.

#### **3.2 Otázka č. 2**

Právna úprava používania elektronického podpisu v Českej republike je príkladom toho, že na národnej úrovni sú priznané rovnocenné účinky s vlastnoručným podpisom aj iným druhom elektronického podpisu ako je kvalifikovaný elektronický podpis. ZSVD priznáva vo vzťahu k verejnému sektoru nad rámec Nariadenia eIDAS právne účinky



vlastnoručného podpisu aj zaručenému (zdokonalenému) elektronickému podpisu, ktorý však musí byť založený na kvalifikovanom certifikáte pre elektronický podpis. V rámci súkromnoprávných vzťahov subjektov je ekvivalentom vlastnoručného podpisu aj obyčajný elektronický podpis.

### 3.3 Otázka č. 3

Zdokonalený elektronický podpis, ktorý spĺňa požiadavky v zmysle Nariadenia eIDAS môže byť ustanovený za uznaný spôsob autorizácie v zmysle ZoEG. Takýto zdokonalený elektronický podpis by mal byť podobne ako v prípade právnej úpravy Českej republiky založený na kvalifikovanom certifikáte pre elektronický podpis, čím sa zaistí jednoznačné spojenie elektronického podpisu s podpisujúcou osobou. Zdokonalený elektronický podpis, ktorý je založený na kvalifikovanom certifikáte pre elektronický podpis spĺňa aj zákonné požiadavky, ktoré sú kladené na uznaný spôsob autorizácie v zmysle ZoEG. Vyhláška upravujúca zdokonalený elektronický podpis ako uznaný spôsob autorizácie, ktorú má prijať MIRR by mala vyslovene určiť, že uznaným spôsobom autorizácie v zmysle § 23 ods. 1 písm. a) bodu 3 ZoEG je zdokonalený elektronický podpis založený na kvalifikovanom certifikáte pre elektronický podpis. V predmetnej vyhláške by prostredníctvom odkazov bolo uvedené, že zdokonalený elektronický podpis, ako aj kvalifikovaný certifikát pre elektronické podpisy musia spĺňať požiadavky podľa Nariadenia eIDAS.

### 3.4 Otázka č. 4

Členské štáty nie sú automaticky povinné uznávať iné formáty elektronických podpisov než tie, ktoré sú uvedené v článku 1 Vykonávacieho rozhodnutia 2015/1506. Táto povinnosť vznikne členským štátom len vtedy ak členský štát, v ktorom má sídlo poskytovateľ dôveryhodných služieb používaný podpisovateľom, ponúkne iným členským štátom možnosti validácie podpisu, ktoré budú podľa možnosti vhodné na automatizované spracovanie. Možnosti validácie podpisu musia spĺňať konkrétne požiadavky v zmysle čl. 2 ods. 2 Vykonávacieho rozhodnutia 2015/1506 a členské štáty by mali prijímajúcim členským štátom poskytnúť ľahko dostupné informácie týkajúce sa týchto validačných nástrojov.