MUNI
LAW

Elektronické dokumenty v praxi

JUDr. Pavel Loutocký, Ph.D., BA (Hons)

Právní úprava

- **Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS)**

- Zákon o službách vytvářejících důvěru pro elektronické transakce (ZSVD)
- Zákon o elektronické identifikaci
- Zákon o elektronických úkonech a autorizované konverzi dokumentů (ZoEU)
- Zákon o archivnictví a spisové službě
- Zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (DEPO)
- Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů

- A další (viz přehled předmětu)

- + kontraktace – zákon č. 89/2012 Sb., občanský zákoník

Obecná nutnost identifikace

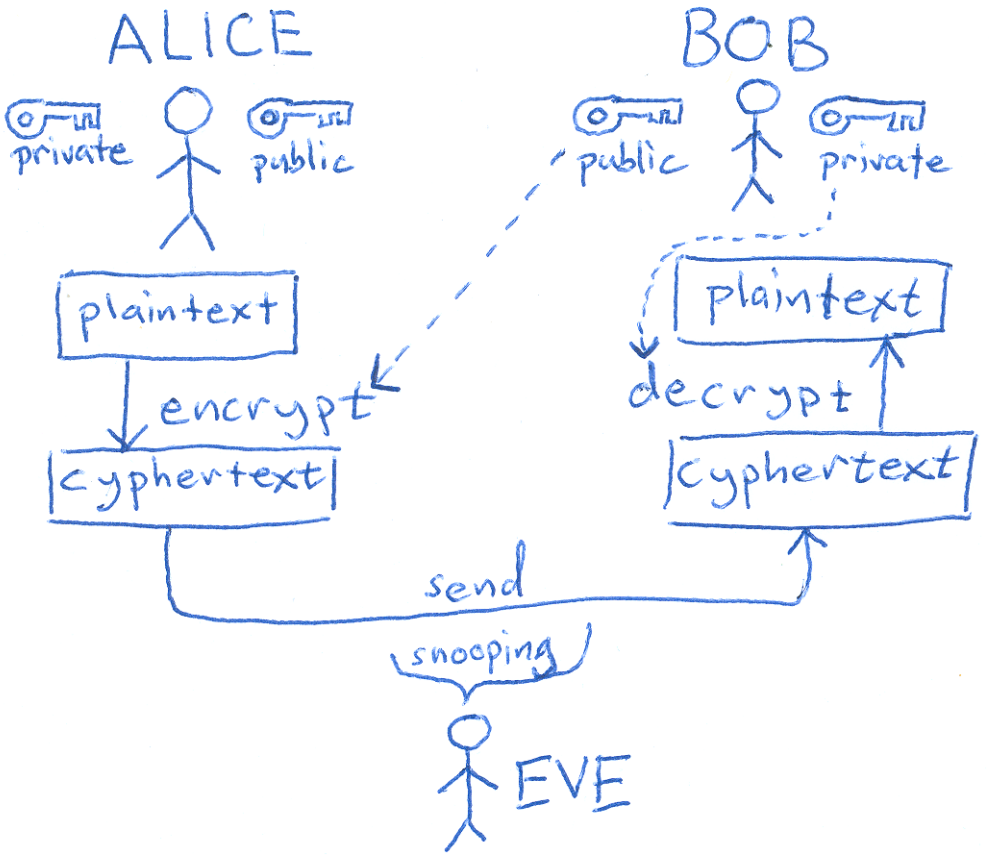
Nutnost odlišit se v rámci právního jednání či při prokazování totožnosti

- e-mailová adresa
- avatar
- uživatelský účet
- IP adresa
- elektronický podpis
- elektronické prokázání totožnost
- …

MUNI LAW

Elektronická identita

Možnosti využití elektronického podpisu byly popsány již v 70. letech 20. století



- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
- UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
- Technicky: https://www.youtube.com/watch?v=Tw5q-SN9ZM8&t=105s

MUNI LAW

Evoluce? Nařízení eIDAS

MUNI LAW

Co znamená nařízení eIDAS

- eIDAS – **e**lectronic **id**entification **a**nd **s**ervices
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- Zveřejněno v Úředním věstníku EU dne 28. 8. 2014

Čeho se nařízení týká?

1. **Oblast elektronické identifikace** (spolupráce, součinnost)

   – „elektronickou identifikací“ se myslí postup používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu (čl. 3 odst. 1 nařízení)

Čeho se nařízení týká?

2. **Oblast služeb vytvářejících důvěru** (sladění úprav)

- služby, které slouží k vytváření důvěry:

  elektronický podpis, elektronická pečeť, elektronické časové razítko

  elektronické doporučené doručování, autentizace internetových stránek

  elektronické dokumenty

Cíle nařízení eIDAS

- Jeden z důležitých nástrojů pro dotvoření digitálního volného vnitřního trhu
- Zvýšení důvěryhodnosti elektronických transakcí v rámci vnitřního trhu
- Vytvoření jednotného rámce pro elektronickou identifikaci jednotlivých subjektů - společný základ pro elektronickou komunikaci mezi občany, podniky a orgány veřejné moci pro efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a elektronického obchodu (obecně dopadá do veřejného i soukromého práva!)
- Nahrazení současné evropské legislativy pro elektronické podpisy a rozšíření působnosti oproti původní směrnici

Působnost nařízení eIDAS

- **Negativní vymezení čl. 2 bod 2, 3**

2. Toto nařízení se nevztahuje na poskytování služeb vytvářejících důvěru, které jsou používány výhradně:
   - v rámci uzavřených systémů dle vnitrostátního práva
   - z dohod mezi určeným okruhem účastníků

3. Tímto nařízením není dotčeno vnitrostátní právo ani právo Unie týkající se:
   - uzavírání a platnosti smluv *(to ale není úplně pravda)*
   - jiných právních nebo procesních povinností týkajících se formy (*to ale není úplně pravda)*

Dopady nařízení eIDAS

- Digitální dokument je rovnocenný listinnému (při dodržení daných podmínek)
- Elektronický podpis je rovnocenný „klasickému“
- Vzájemné uznávání a umožnění využívání elektronické identifikace a doručování
- Certifikované služby pro vytváření, ověřování a udržování podpisů, pečetí a časových razítek

Dopady nařízení eIDAS

- Na „národní úroveň“ je ponecháno:
  - stanovení sankcí za nedodržení různých požadavků
  - případné přestupky
  - určení národních orgánů dohledu nad poskytovateli služeb vytvářejících důvěru
  - atd.

Role Evropské Komise

- Přijímá oznámení prostředků pro elektronickou identifikaci
- Stanoví minimální technické specifikace, normy a postupy pro vymezení jednotlivých úrovní zabezpečení (nízká, značná a vysoká)
- Ověřuje způsobilost systémů elektronické identifikace
- Spolupracuje se členskými státy při narušení bezpečnosti
- Vydává další prováděcí akty k eIDAS

Prováděcí akty k nařízení eIDAS

- https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/legislativa/
- **Například:**
  - Rozhodnutí 2015/296 z 24.2.2015 - procesní opatření pro spolupráci mezi členskými státy v oblasti elektronické identifikace
  - Nařízení 2015/806 z 22.5.2015 - specifikace značky důvěry EU pro kvalifikované služby vytvářející důvěru
  - Nařízení 2015/1502 z 8.9.2015 - minimální technické specifikace a postupy úrovně záruky prostředků pro elektronickou identifikaci podle čl. 8/3 eIDAS
  - Rozhodnutí 2015/1506 z 8.9.2015 - specifikace zaručených elektronických podpisů a pečetí uznávaných subjekty veřejného sektoru podle čl. 27/5 a 37/5 eIDAS

Konkrétní legislativní dopady v ČR

1. zákon 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce (doplnění národní právní úpravy k podpisům/pečetím/časovým razítkům k nařízení eIDAS)
2. zákon 250/2017 Sb., o elektronické identifikaci (unifikace systému, elektronické prokazování totožnosti)

1. Oblast elektronické identifikace

- Uznávání elektronické identity FO nebo PO, která byla přidělena v jiném členském státě
- Neznamená to ale jednotnou „evropskou elektronickou identitu“
- FO nebo PO bude uznávána elektronická identita přidělena v „jejím“ státě přímo bez toho, aniž by jí musela být přidělena identita v tom státě, kde má být identita uznána
- eID / totožnost (nutno odlišovat od podpisů, ale někdy se projevy směrem k právnímu jednání prolínají)

1. Oblast elektronické identifikace

- 3 úrovně prostředků pro elektronickou identifikaci (tzv. úrovně důvěry):
  1. **Nízká:** jméno, heslo
  2. **Značná:** certifikát pro autentizaci
  3. **Vysoká:** certifikát pro autentizaci uložený na elektronickém identifikačním průkazu/jiném zabezpečeném úložišti
- STORK 2.0 (**S**ecured Iden**t**ity Acr**o**ss Bo**r**ders Lin**k**ed)

1. Oblast elektronické identifikace

- Prováděcí akt, technické specifikace, normy a postupy
- Členské státy stanoví, jestli do elektronické identifikace pro přístup k online službám zapojí i soukromý sektor
- Akreditace v ČR:

  https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/

- EU notifikovaná schémata:

  https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

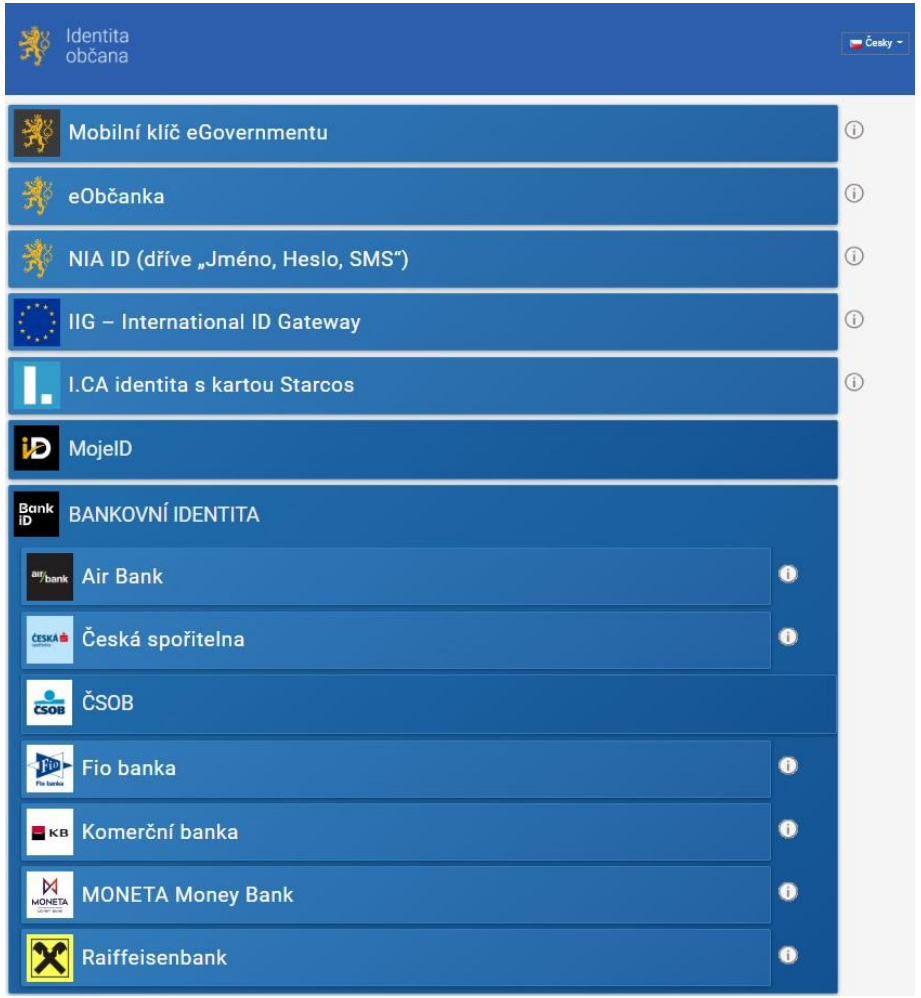
MUNI LAW

Zákon 250/2017 Sb., o elektronické identifikaci

- upraven obecný institut elektronické identifikace + kvalifikované systémy
- stanovení pravidel pro jednotlivé strany, které se účastní procesu elektronické identifikace
- jedná se o doplnění legislativy, který propojuje nutnost/možnost identifikace s elektronickou identifikací (eID)

Příklad

- Mnoho identit a možností přístupu
- Nový potenciál bankovní identity...
- **Silně roztříštěné...**



MUNI LAW

Bankovní identita vs. BankID

- využití bankovní identity k přístupu ke službám veřejné správy (a BankID také v rámci soukromého sektoru / kontraktace)
- Akreditace nutná, jelikož bankovní identita se napojuje na základní registry (bankám udělen přístup k základním registrům (např. registr obyvatel, informační systém cizinců), veškeré informace o jejich klientech se tak aktualizují)

- https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/povinne-zverejnovane-informace/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru/

Evropská digitální identita

- **Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu**

- ***Aktuálně se předpokládá, že text eIDAS2 by mohl být zveřejněn cca v dubnu příštího roku, takže při započítání dalších lhůt by povinnost vydávat peněženky pro členské státy měla nastat cca koncem roku 2026.***

- *(https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A32014R0910)*

Evropská digitální identita

- „*Evropskou digitální identitu budou moci využívat občané, rezidenti a podniky v EU, kteří chtějí prokázat svou identitu nebo potvrdit určité osobní informace. Lze ji využít online i offline u veřejných i soukromých služeb v celé EU.*“ (https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_cs)

- Ústředním bodem je Evropská peněženka digitální identity (ústřední nástroj Evropského rámce digitální identity).

- *Toto nařízení se vztahuje na systémy elektronické identifikace oznámené členskými státy, na evropské peněženky digitální identity vydané členskými státy a na poskytovatele služeb vytvářejících důvěru usazené v Unii.* (čl. 2/1 návrhu nařízení)

Evropská digitální identita

Evropskou digitální identitu lze využívat různým způsobem, například:

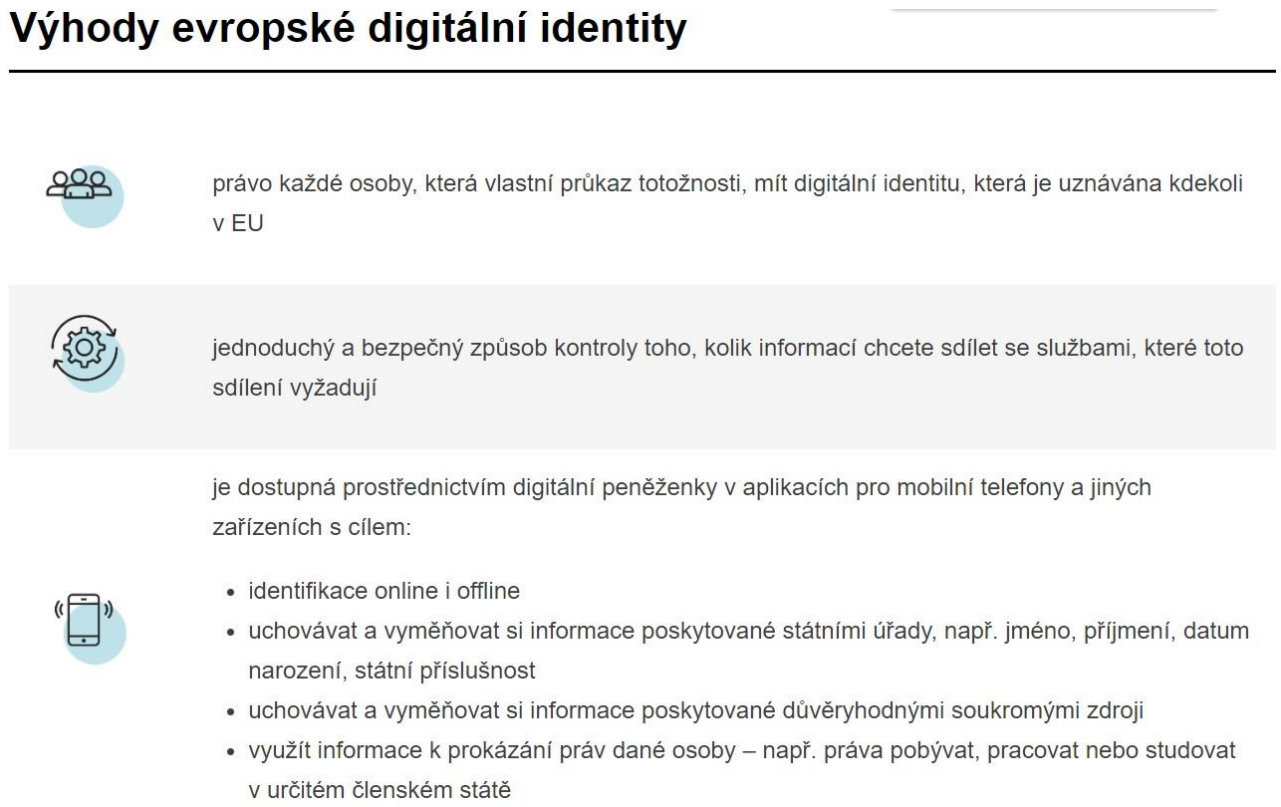
- *u veřejných služeb, jako jsou žádosti o vydání rodného listu, lékařského potvrzení nebo nahlášení změny adresy*
- *k otevření bankovního účtu*
- *k podávání daňového přiznání*
- *při předkládání přihlášky na univerzitu, doma nebo v jiném státě Unie*
- *k uložení lékařského předpisu, který lze použít kdekoli v EU*
- *k prokázání věku*
- *při pronajímání vozidla pomocí digitálního řidičského průkazu*
- *při ubytování v hotelu*

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_cs

Evropská digitální peněženka

- Digitální peněženka bude sdružovat různé nástroje pro identifikaci (nejen kvalifikované služby).

- *Z průzkumu Eurobarometru vyplývá, že 72 % uživatelů chce vědět, jakým způsobem zpracovávají jejich údaje sociální média. 63 % občanů EU si přeje bezpečnou jednotnou digitální identifikaci pro všechny online služby.*



MUNI LAW

Evropská digitální peněženka

- „evropskou peněženkou digitální identity“ produkt a služba, které uživateli umožňují uchovávat údaje o totožnosti, pověření a atributy spojené s jeho totožností, poskytovat je na požádání spoléhajícím se stranám a používat je pro autentizaci, on-line i offline, pro službu v souladu s článkem 6a; a k vytváření kvalifikovaných elektronických podpisů a pečetí;

- Spoléhající se strany („*Pokud mají spoléhající se strany v úmyslu spoléhat se na evropské peněženky digitální identity vydané v souladu s tímto nařízením, sdělí to členskému státu, v němž je spoléhající se strana usazena…*“ čl. 6b)
- Certifikace
- Seznamy certifikovaných poskytovatelů

Atributová autentizace jako zajímavost

- Je ale vždy potřeba ověřovat identitu?
- Atributové systémy, jako minimalizace nakládání s osobními údaji a optimalizace zatížení a nastavení organizačních a právních pravidel
- Skupinové přístupy, skupinová oprávnění, potvrzení o vlastnosti

2. Oblast služeb vytvářejících důvěru

– Elektronická služba, která je zpravidla poskytována za úplatu (čl. 3 odst. 16)

- elektronický podpis, elektronická pečeť, elektronické časové razítko
- elektronické doporučené doručování, autentizace internetových stránek
- elektronické dokumenty
- uchovávání elektronických podpisů a pečetí (tzv. digitální kontinuita)

Elektronický podpis dle čl. 3/10 eIDAS

- data v elektronické podobě,
- která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena
- a která podepisující osoba používá k podepsání

- Zaručený elektronický podpis umožňuje jednoznačnou identifikaci podepisující osoby

Tedy znovu!
Co je elektronický podpis?

JUDr. Pavel Loutocký, Ph.D., BA(Hons)

Digitálně podepsal JUDr. Pavel Loutocký, Ph.D., BA(Hons)
Datum: 2024.03.12 15:26:13 +01'00'

MUNI LAW

Základní potenciální funkce

1. Vyjádření souhlasu
2. Potenciálně identifikace osoby
3. Potenciálně integrita dokumentu

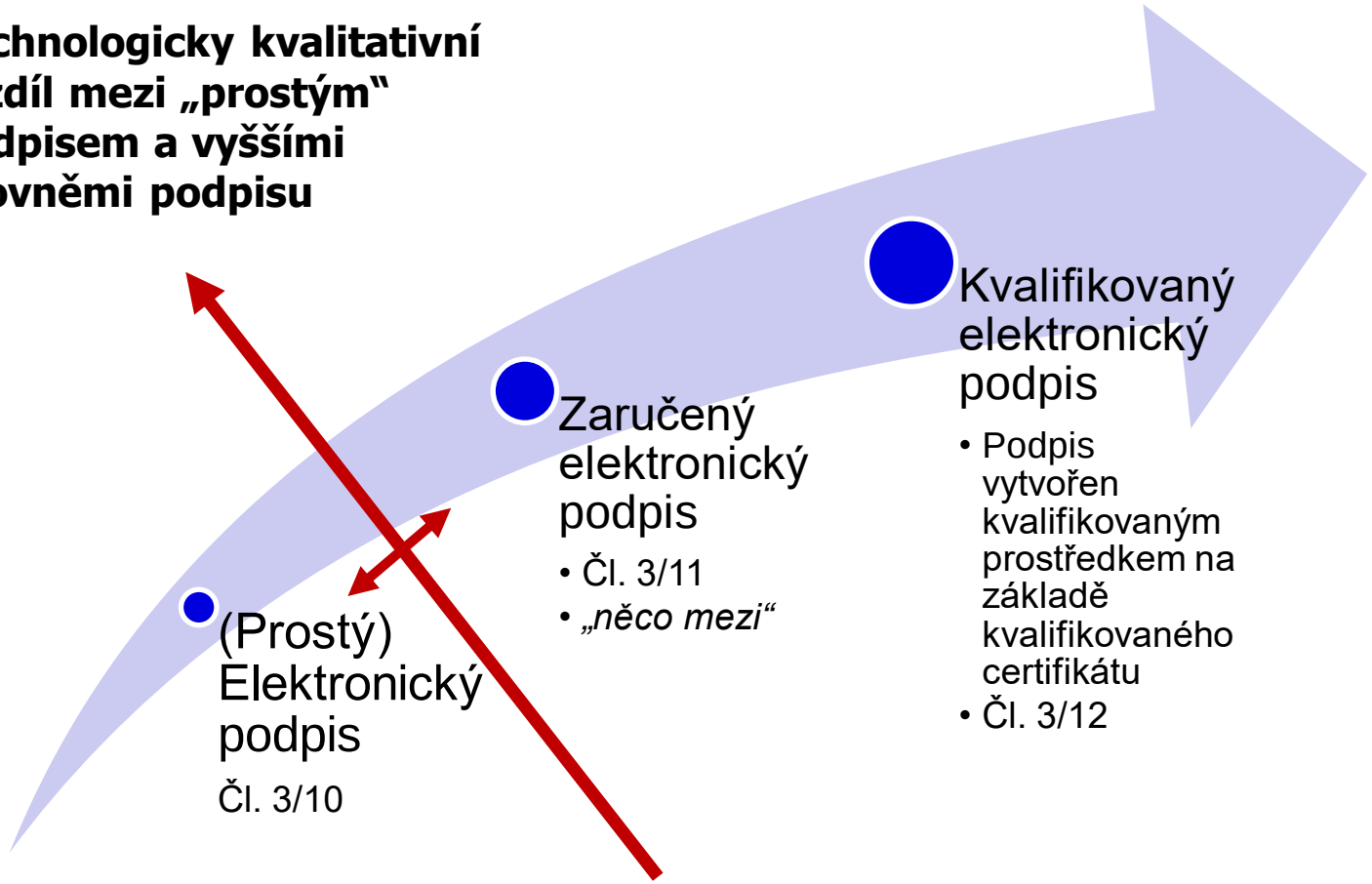
- (jiné dopady oproti podpisu „na papíře“)

čl. 25 EIDAS

1. Elektronickému podpisu **nesmějí být upírány právní účinky** a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.
2. **Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu**.
3. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě **se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech**.

Druhy elektronických podpisů dle eIDAS

Technologicky kvalitativní rozdíl mezi „prostým" podpisem a vyššími úrovněmi podpisu



Právně má každá úroveň odlišnou důkazní spolehlivost

MUNI LAW

Druhy elektronických podpisů dle eIDAS

„Prostý“ elektronický podpis

- cokoli, co nějakým způsobem identifikuje subjekt a je připojeno k jiným datům

Zaručený elektronický podpis

- je založen na certifikátu, ale na ten nejsou kladeny žádné požadavky – může jít i o testovací certifikát (ten může obsahovat jakoukoli informaci)

Kvalifikovaný elektronický podpis

- musí být založen na kvalifikovaném certifikátu pro elektronický podpis a musí být vytvořen pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů (např. čipové karty – eID nebo tokeny)

Příklady druhů elektronického podpisu dle eIDAS

1) „prostý“ elektronický podpis

JUDr. Pavel Loutocký, Ph.D., BA (Hons)
Masarykova univerzita / Masaryk University

– **Dle OZ navíc úvahy nad „** prostředky umožňujícími zachycení jeho obsahu a **určení jednající osoby“ – osoba může být určena i jinak než podpisem – úmysl zákonodárce? (IP adresa? hash identifikátor? …)**

MUNI LAW

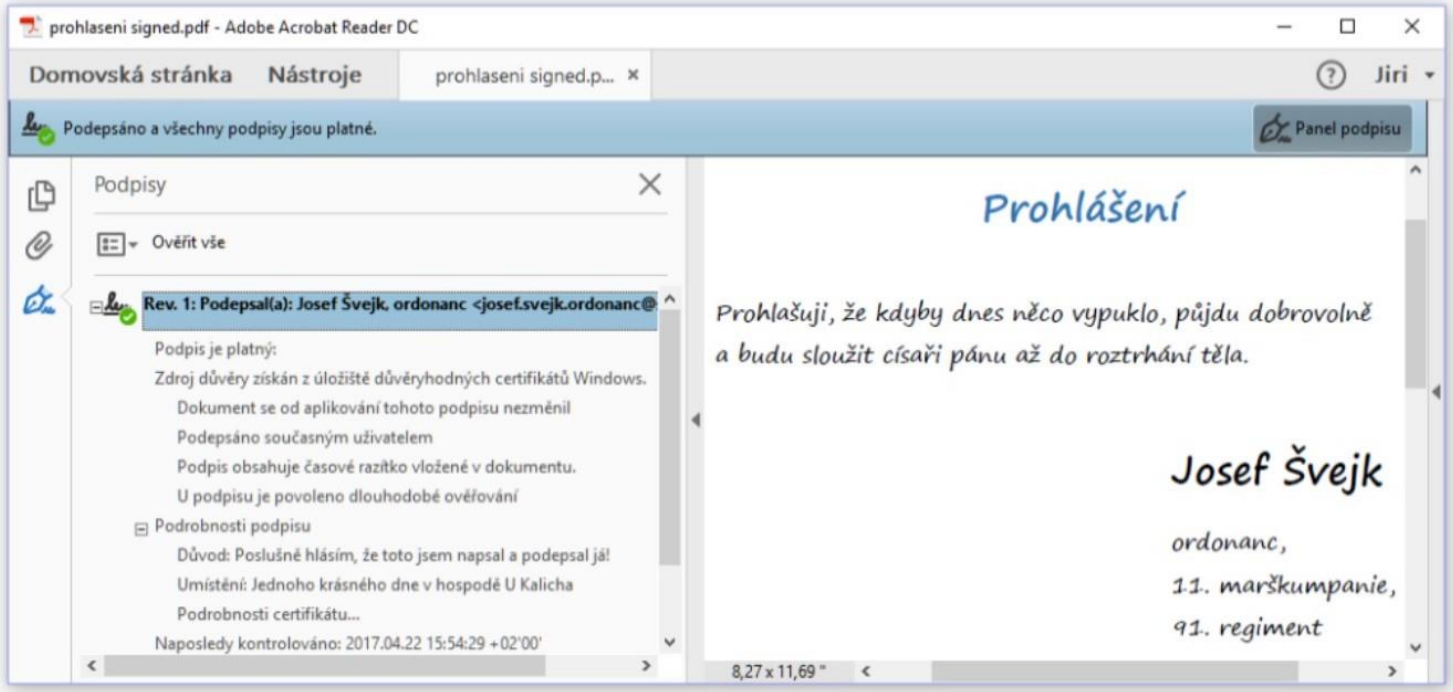
Zaručený elektronický podpis – čl. 26

- Zaručený elektronický podpis musí splňovat tyto požadavky:
  a) je jednoznačně spojen s podepisující osobou;
  b) umožňuje identifikaci podepisující osoby;
  c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a
  d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

Příklady druhů elektronického podpisu dle eIDAS

– **zaručený elektro**

příklad zaručeného el. podpisu



- **pozor: zaručený el. podpis nezaručuje identitu podepsané osoby !!!**
  - formou zaručeného elektronického podpisu se lze (velmi snadno) podepsat za kohokoli jiného
  - zaručený podpis může „patřit“ i někomu, kdo vůbec neexistuje (jako fyzická osoba)
- **zaručuje pouze neměnnost (integritu) toho, co je podepsáno ....**

MUNI LAW

Příklady druhů elektronického podpisu dle eIDAS

- kvalifikovaný elektronický podpis

- … nasdílím příklad

Kvalifikovaný elektronický podpis

- Kvalifikovaný (eIDAS) = uznávaný (starý zákon o el. podpisu)
- Čl. 28 a násl. nařízení eIDAS
  - Kvalifikované certifikáty
  - Požadavky kladené na certifikáty
  - Certifikace a postupy
  - Zveřejnění seznamu certifikačních prostředků
  - Požadavky na ověřování certifikátu
  - kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů
  - kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů

Kvalifikovaný elektronický podpis (dle čl. 3 eIDAS)

- „**kvalifikovaným elektronickým podpisem**“ zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy;
- „**kvalifikovaným certifikátem pro elektronický podpis**“ certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje požadavky stanovené v **příloze I**
- „**kvalifikovaným prostředkem pro vytváření elektronických podpisů**“ prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v **příloze II**

Kvalifikovaný elektronický podpis – Příloha I

Kvalifikované certifikáty pro elektronické podpisy obsahují:

a) **označení**, …, že se certifikát vydává jako kvalifikovaný certifikát pro elektronický podpis;

b) **soubor dat jednoznačně identifikujících kvalifikovaného poskytovatele služeb** vytvářejících důvěru…;

c) alespoň **jméno podepisující osoby nebo pseudonym**. Je-li použit pseudonym, musí být tato skutečnost jasně vyznačena;

d) **data pro ověřování platnosti elektronických podpisů**…;

e) **označení začátku a konce doby platnosti** certifikátu;

f) **identifikační číslo** certifikátu;

g) zaručený elektronický podpis nebo zaručenou elektronickou pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru, který certifikát vydává;

h) údaj o místu, kde je bezplatně k dispozici certifikát, na němž je založen zaručený elektronický podpis nebo zaručená elektronická pečeť podle písmene g)

i) **údaj o umístění služeb, které lze využít k zjištění platnosti kvalifikovaného certifikátu**;

j) …

Kvalifikovaný elektronický podpis – Příloha II

1. Kvalifikované prostředky pro vytváření elektronických podpisů vhodnými technickými prostředky a postupy přinejmenším zajistí, aby:

a) **byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů**, která byla použita při vytváření elektronického podpisu;

b) data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu se mohla **prakticky vyskytnout pouze jednou**;

c) bylo přiměřeně zajištěno, že data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu **nelze odvodit a že elektronický podpis je v současnosti dostupnými technickými prostředky spolehlivě chráněn proti padělání**;

d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu **spolehlivě chránit před jejich zneužitím třetí osobou**.

2. Kvalifikované prostředky pro vytváření elektronických podpisů **nesmějí měnit podepisovaná data** ani bránit tomu, aby byla tato data předložena podepisující osobě před vlastním podepsáním.

3. Data pro vytváření elektronických podpisů **může jménem podepisující osoby vytvářet nebo spravovat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru**.

MUNI LAW

Kvalifikovaný elektronický podpis – Příloha II

Seznam vydávaných kvalifikovaných prostředků pro vytváření elektronických podpisů v České republice:

https://www.dia.gov.cz/egovernment/eidas-sluzby-vytvarejici-duveru-a-elektronicka-identifikace/

MUNI LAW

Kvalifikovaný elektronický podpis

Remote sign? – serverová řešení, mobilní řešení

eIDAS:

Bod odůvodnění 51) *Podepisující osoba by měla mít možnost svěřit kvalifikované prostředky pro vytváření elektronických podpisů do péče třetí straně, pokud jsou zavedeny odpovídající mechanismy a postupy, které zajišťují, že podepisující osoba má výhradní kontrolu nad používáním svých dat pro vytváření elektronických podpisů, a použitím tohoto prostředku jsou splněny požadavky na kvalifikovaný elektronický podpis.*

Bod odůvodnění 52) *Vytváření elektronického podpisu na dálku, jehož prostředí spravuje poskytovatel služeb vytvářejících důvěru jménem podepisující osoby, přináší mnohé ekonomické výhody, a bude tedy pravděpodobně stále častější. Aby však bylo zajištěno, že tyto elektronické podpisy budou z právního hlediska uznávány stejně jako elektronické podpisy, které jsou vytvářeny v prostředí spravovaném výlučně uživatelem, měli by poskytovatelé nabízející služby elektronického podpisu na dálku uplatňovat zvláštní postupy pro zajištění bezpečnosti v oblasti řízení a správy a používat důvěryhodné systémy a produkty zahrnující zabezpečené kanály pro elektronickou komunikaci, a zajistit tak spolehlivost prostředí, v němž jsou elektronické podpisy vytvářeny, a zaručit, že je toto prostředí používáno pod výlučnou kontrolou podepisující osoby. V případě kvalifikovaného elektronického podpisu vytvořeného pomocí prostředku pro vytváření elektronických podpisů na dálku by se měly použít požadavky stanovené v tomto nařízení, které jsou použitelné na kvalifikované poskytovatele služeb vytvářejících důvěru.*

MUNI LAW

Kvalifikovaný vs uznávaný elektroncický podpis

- **Kvalifikovaný elektronický podpis**
- Zaručený podpis založený na kvalifikovaném certifikátu a vytvořen kvalifikovanými prostředky pro vytváření elektronických podpisů (QSCD)

X

- **Uznávaný elektronický podpis (původně)**
- zaručený elektronický podpis založený na kvalifikovaném certifikátu

X

- Pojem „uznávaný elektronický podpis“ ale označuje dle ZSVD jednak kvalifikovaný el. podpis, tak i zaručený elektronický podpis, založený na kvalifikovaném certifikátu

Perlička v zaměňování pojmů

- **Stará právní úprava (příklad z minulosti)**

- Uznávaný el. podpis vždy při komunikaci s veřejnou správou (soudy, atp.)

X

- § 174a odst. 6 OSŘ
- **(6)** Odpor proti elektronickému platebnímu rozkazu lze podat také na elektronickém formuláři podepsaném zaručeným elektronickým podpisem.

- Chyba??

Elektronický podpis a legalizace

- V ČR chyběla úprava úředního ověření elektronického podpisu; činilo se to (nesystémově, ale prakticky) zvláštními předpisy, např.:
  - *§ 97/2 IZ: Insolvenční návrh musí být v listinné podobě opatřen* ***úředně ověřeným podpisem*** ~~*nebo v elektronické podobě* ***uznávaným elektronickým podpisem****, nebo zaslán prostřednictvím její* ***datové schránky***~~*…* zrušeno z. č. 298/2016 Sb.!
  - *§ 22/2, 3 RZ: Podpis na návrhu na zápis v listinné podobě musí být* ***úředně ověřen****. Návrh na zápis v elektronické podobě musí být podepsán* ~~*uznávaným* ***elektronickým podpisem*** *podle zákona upravujícího elektronický podpis nebo zaslán prostřednictvím* ***datové schránky***~~ *způsobem, se kterým jiný právní předpis spojuje účinky vlastnoručního podpisu (§ 18/2 ZEU, § 6/1 ZSVDET)*
  - *§ 10/12 zákona o evidenci obyvatel (oznamování ohlašovně)*
  - A

MUNI LAW

Elektronický podpis a legalizace

– § 7 z. č. 256/2013 Sb., o katastru nemovitostí (katastrální zákon)

(1) Zápisy práv se do katastru provádějí na základě písemností v listinné podobě nebo v elektronické podobě (dále jen "listina").

- Pokud je listina vyhotovena v elektronické podobě, musí být též opatřena **kvalifikovaným elektronickým časovým razítkem**.
- Je-li listina v elektronické podobě podepsána elektronickým podpisem, musí být k podepsání použit **uznávaný elektronický podpis**.
- Je-li písemnost v elektronické podobě zapečetěna elektronickou pečetí, musí být k pečetění použita **uznávaná elektronická pečeť**.

(2) Nejsou-li podpisy na soukromé listině úředně ověřeny, musí ten, kdo zápis navrhuje, prokázat jejich pravost.

Elektronický podpis a legalizace

– Zákon o právu na digitální služby

§ 6 (od 1.2.2022)

- **Právo na nahrazení úředně ověřeného podpisu nebo uznávaného elektronického podpisu**
- **(1)** Stanoví-li právní předpis požadavek úředního ověření vlastnoručního podpisu nebo uznávaného elektronického podpisu, považuje se za splněný využitím elektronického podpisu na dokumentu nedílně spojeném
  - **a)** s **kvalifikovaným elektronickým podpisem** osoby oprávněné provádět ověřování pravosti podpisu, která postupem podle jiného právního předpisu[8)] ověřila, že podepisující dokument před ní podepsal nebo uznal podpis za vlastní, a kvalifikovaným elektronickým časovým razítkem, nebo
  - **b)** se **záznamem informačního systému veřejné správy** opatřeným kvalifikovanou elektronickou pečetí a kvalifikovaným elektronickým časovým razítkem jeho správce o provedení elektronické identifikace podepisujícího prostřednictvím kvalifikovaného systému elektronické identifikace s úrovní záruky vysoká.
- **(2)** Stanoví-li právní předpis požadavek úředního ověření podpisu, považuje se za splněný využitím **uznávaného elektronického podpisu**, pokud lze s využitím údajů základního registru obyvatel (dále jen „registr obyvatel“) nebo portálu veřejné správy ověřit, že kvalifikovaný certifikát pro elektronický podpis, na jehož základě podepisující vytvořil uznávaný elektronický podpis na dokumentu, patří podepisujícímu.
- **(3)** Ustanovení § 6 odst. 1 písm. b) a § 6 odst. 2 se nepoužijí pro plnou moc k právnímu jednání podle § 441 odst. 2 poslední věty občanského zákoníku.

- …. Usnesení Vrchního soudu v Praze - 3 VSPH 610/2023-A-122

MUNI LAW

Autority pro kvalifikované podpisy v ČR

- První certifikační autorita, a. s.,
- Česká pošta, s. p.
- eIdentity a. s.

Nově:

- Komerční banka, a.s. (6/2023)
- Správa státních služeb vytvářejících důvěru (11/2023) - příspěvková organizace DIA

Jak získat kvalifikovaný el. podpis/pečeť/razítko

- https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists
- http://www.postsignum.cz/fyzicke_osoby.html

Jak ověřit platnost elektronického podpisu nebo pečeti jako kvalifikované

V PDF (jak bylo prezentováno)

Nebo dle návodu zde: https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/How+do+I+validate+an+electronic+signature+or+seal+as+qualified (nutno se ale zaregistrovat…)

MUNI LAW

Elektronická pečeť

- Speciální typ elektronického podpisu
  - Bez úzké vazby na „podepisující“ osobu
  - Reprezentuje PO

- Dle eIDAS (čl. 3/25)
  - Opět „data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu“

Elektronická pečeť

1. „Prostá" elektronická pečeť
2. Zaručená elektronická pečeť
3. Kvalifikovaná elektronická pečeť (+ zaručená, založená na kvalifikovaném certifikátu)

- jejím cílem je potvrdit neporušenost zapečetěného dokumentu a jeho původ, nikoli vůli (právnické) osoby.
- Příklady: potvrzení o přijetí dokumentu v rámci spisové služby, výstupy z informačního systému veřejné správy.

Elektronické časové razítko

Čl. 3/33 eIDAS

- „elektronickým časovým razítkem“ jsou data v elektronické podobě, která spojují jiná data v elektronické podobě s určitým okamžikem a prokazují, že tato jiná data existovala v daném okamžiku;

Elektronické časové razítko

- dokazuje, že elektronický dokument, ke kterému bylo razítko připojeno, v daném okamžiku existoval.
- jiné nástroje - podpis nebo pečeť - nejsou schopny tuto skutečnost spolehlivě prokázat.
- Lze jej spojit s elektronickým podpisem (pečetí) a nabídnout tak "jeden" nástroj k podepisování (zajištění integrity) a prokazování času (zpravidla pak platnost takto spojeného certifikátu po delší dobu)

Kvalifikované elektronické časové razítko (čl. 42 eIDAS)

a) spojuje datum a čas s daty takovým způsobem, aby byla přiměřeně zamezena možnost nezjistitelné změny dat;

b) je založeno na zdroji přesného času, který je spojen s koordinovaným světovým časem; a

c) je podepsáno s použitím zaručeného elektronického podpisu, opatřeno zaručenou elektronickou pečetí kvalifikovaného poskytovatele služeb vytvářejících důvěru nebo označeno jinou rovnocennou metodou.

Pravidla podepisování dokumentu

(Zákon 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce)

1. Dokument podepisuje veřejný orgán – vždy nutnost podepsat kvalifikovaným elektronickým podpisem (§ 5)
2. V případě podepisování dokumentu soukromou osobou v případě komunikace s veřejným orgánem – uznávaný elektronický podpis (§ 6)
3. Mimo výkon veřejné moci - jakýkoli podpis (§ 7)

Pravidla pečetění dokumentu

- Veřejnoprávní „pečetící“ vs. okolí (§ 8)
  - kvalifikovanou elektronickou pečetí

- Soukromá osoba pečetí směrem k veřejnoprávnímu subjektu (§ 9)
  - Kvalifikovaná elektronická pečeť, zaručená el. pečeť založená na kvalifikovaném certifikátu
- Pečetění jiných dokumentů (§ 10)
  - Jakákoli jiná pečeť

Doporučené doručování – čl. 36 eIDAS

- „službou elektronického doporučeného doručování“ 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;

- Na této obecné úrovni lze předpokládat, že tyto požadavky budou splňovat různé systémy doručování schopné vytvářet spolehlivé protokoly a záznamy o různých činnostech, které se provádějí při manipulaci s elektronickými dokumenty.
- … a mj. tedy datové schránky

Kvalifikované doporučené doručování

- Kvalifikované elektronické doporučené doručování musí být zajišťováno kvalifikovaným poskytovatelem služeb; musí umožňovat identifikaci odesílatele i příjemce s vysokou mírou spolehlivosti; samotné odeslání je zabezpečeno zaručeným elektronickým podpisem tak, aby bylo možné zjistit změny údajů (pokud k nim dojde, musí být informován odesílatel i příjemce); čas odeslání je pak označen kvalifikovaným elektronickým časovým razítkem atd. (čl. 44 eIDAS).

- Je přístupné např. v Belgii, Itálii, Německu, Španělsku, Francii, Nizozemsku, Polsku a Slovinsku.

Autentizace webových stránek

- „certifikátem pro autentizaci internetových stránek“ potvrzení, které umožňuje autentizovat internetové stránky a spojuje je s fyzickou nebo právnickou osobou, jíž je certifikát vydán (čl. 3/36 eIDAS)
- U kvalifikovaných služeb musí být certifikát vydán kvalifikovaným poskytovatelem a musí splňovat specifické požadavky, jako je údaj o zabezpečení webové stránky a spojení s osobou, které byl certifikát vydán (včetně ověření pravosti), informace o organizaci a certifikační autoritě, která certifikát vydala, název certifikované domény nebo doba platnosti certifikátu.
- Není příliš využíváno - je to pravděpodobně způsobeno tím, že použití tohoto nástroje nepřináší mnoho výhod oproti jiným, tradičně zavedeným nástrojům (často poskytovaným společnostmi mimo EU), proces vydávání kvalifikovaných certifikátů je procesně složitější a jedná se o dobrovolný nástroj.

Uchovávání kvalifikovaných elektronických podpisů

Čl. 34 nařízení eIDAS

- kvalifikovaný poskytovatel služeb vytvářejících důvěru, který používá postupy a technologie, jež jsou s to zajistit důvěryhodnost kvalifikovaného elektronického podpisu i po uplynutí doby technické platnosti

- Co to znamená?

1. Kontrola platnosti certifikátů – je el. podpis ještě platný?
2. Nedošlo k jeho zneplatnění?

Uchovávání = Archivace?

- Nařízení archivaci el. dokumentů komplexně neřeší!

Recitál 61

- *Toto nařízení by mělo zajistit dlouhodobé uchovávání informací, aby zajistilo dlouhodobou platnost elektronických podpisů a elektronických pečetí a zaručilo, že mohou být ověřeny bez ohledu na budoucí technologické změny.*

Neřeší archivaci ale tak jako české právo („přerazítkováváním“ dokumentu)

+ čl. 34 - Kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů

Archivace?

1. **Přerazítkování**
   - **Věrohodnost původu** – totožnost osoby
   - **Neporušenost obsahu** – obsah nebyl změněn
   - **Čitelnost** – je možné se seznámit s obsahem
   - V rámci archivu dochází po cca roce k přerazítkování (řetěz důvěry)

2. **Elektronické zabezpečovací prvky**
   - Obdobně jako přerazítkovávání, ale soukromě

3. **Transakční protokol**
   - Ukládání protokolu např jednou denně, připojení kvalifikovaného razítka a podpisu/pečetě

4. **Důvěryhodný repozitář**
   - Specifické nástroje pro zajištění důvěryhodnosti – využití transakčního protokolu a dalších nástrojů pro archivaci – logování atp.
   - § 562/2 OZ

MUNI LAW

Archivace?

- Uchovávání el. dokumentů – webová stránka - **rozsudek Nejvyššího správního soudu sp. zn. 1 As 80/2016-30**

- **„***zachycení obsahu stránky musí být provedeno tak, aby relevantní grafické prvky nebyly deformovány či eliminovány.* […]*Způsob zachycení obsahu internetových stránek předurčuje rovněž to, zda je předmětem dokazování otázka, zda konkrétní informace s konkrétním obsahem na stránkách publikována byla (např. zda byl na internetu publikován dehonestující článek), anebo je předmětem dokazování absence určité informace na internetové stránce (např. právě neuvedení povinných náležitostí reklamy). Zatímco v prvním případě by vytištění internetové stránky dokumentující pouze existenci prokazované skutečnosti dostačovalo, ve druhém případě je třeba zachytit podobu internetové stránky komplexněji. Je třeba zdokumentovat všechny prvky internetové stránky, které by reálně byly schopné nést určité sdělení, které na stránkách má absentovat.* **“**

- *„Při zachycení obsahu internetové stránky pouze tiskem může dojít ke ztrátě některých grafických prvků, které mohou obsahovat plnohodnotný text.“*

Datové schránky

- Způsob doručování písemností ve veřejné správě
- Povinnost orgánů veřejné moci komunikovat výhradně prostřednictvím tohoto systému

Datové schránky vs. email?

MUNI
LAW

Datové schránky vs. email?

- Obě jsou elektronickým úložištěm
- Datová schránka ale není kompatibilní s emailem
- Na rozdíl od emailu garantuje doručení ve smyslu zákona (správní řád, atd.)

Datové schránky

Zákon 300/2008 Sb.

- § 2 Datová schránka
- (1) Datová schránka je elektronické úložiště, které je určeno k
  - a) doručování orgány veřejné moci,
  - b) provádění úkonů vůči orgánům veřejné moci,
  - c) dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.
- (2) Datové schránky zřizuje a spravuje Digitální a informační agentura (dále jen „Agentura“).

Zákony

- Zákon č. 500/2004 Sb., správní řád
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů (ZoEU)
- Vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů
- Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek

Způsoby komunikace

1. Orgán veřejné moci - Orgán veřejné moci
2. Orgán veřejné moci - Občan
3. Občan – Občan

Operace datových schránek

- odesílat zprávy
- přijímat zprávy
- zjišťovat stavy odeslaných zpráv
- přijímat doklady o dodání a doručení
- ověřovat, zda adresát má datovou schránku

Datové schránky

- Ze zákona
  - Orgány veřejné moci
  - Právnické osoby zřízeny zákonem
  - Právnické osoby zapsané v OR
  - Právnické osoby obecně
  - Fyzické osoby podnikatelé

- Na žádost
  - Fyzické osoby (ale nemělo to tak původně být)

  - Viz od 1.1.2023: zákon č. 261/2021 Sb., zákon, kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci (tzv. DEPO)

Orgány veřejné moci

- státní orgány
- orgány územních samosprávných celků
- Pozemkový fond České republiky
- státní fondy
- zdravotní pojišťovny
- Český rozhlas
- Česká televize
- samosprávné komory zřízené zákonem,
- notáři
- soudních exekutoři

§ 17/1 ZoEU - Doručování

- **Umožňuje-li to povaha dokumentu**, orgán veřejné moci jej doručuje jinému orgánu veřejné moci prostřednictvím datové schránky, pokud se nedoručuje na místě.
- **Umožňuje-li to povaha dokumentu** a má-li fyzická osoba, podnikající fyzická osoba nebo právnická osoba zpřístupněnu svou datovou schránku, orgán veřejné moci doručuje dokument této osobě prostřednictvím datové schránky, pokud se nedoručuje veřejnou vyhláškou nebo na místě. Doručuje-li se způsobem podle tohoto zákona, ustanovení jiných právních předpisů upravující způsob doručení se nepoužijí

§ 17/4 ZoEU – Fikce doručení

– *Nepřihlásí-li se do datové schránky osoba podle odstavce 3 ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručený posledním dnem této lhůty; to neplatí, vylučuje-li jiný právní předpis náhradní doručení.*

Praktické následky fikce

- Faktická povinnost pravidelně přistupovat do datové schránky
- Zefektivnění procesů ve veřejné správě
- Doručení se fakticky není možné vyhnout
  - Zrychlení řízení s větším počtem účastníků

- **Dodání** - den, kdy je datová zpráva dostupná v datové schránce
- **Doručení** - den přístupu k datové zprávě (resp. přihlášení)
- **Dodání = doručení** - u orgánů veřejné správy

Doručování prostřednictvím datových schránek

- Vkládání dokumentů
- Pouze v autorizovaných formátech
  - 194/2009 – O užívání a provozování datových schránek
  - § 4 (**které to jsou?**)
  - https://www.zakonyprolidi.cz/cs/2009-194

Informační systém datových schránek - údaje

§ 14 odst. 3 ZeEU

a) identifikátor datové schránky (dále jen „identifikátor“),
b) datum zřízení, zpřístupnění, znepřístupnění a zrušení
c) datum přihlášení osoby oprávněné k přístupu do datové schránky
d) datum odeslání dokumentu nebo provedení úkonu z datové schránky s uvedením hodiny, minuty a sekundy a údaj identifikující osobu, která odeslání dokumentu nebo úkon provedla,
e) jméno, fyzické osoby, pro niž byla zřízena datová schránka,
f) jméno popřípadě obchodní firma podnikající fyzické osoby, pro niž byla zřízena datová schránka,
g) obchodní firma nebo název právnické osoby, pro niž byla zřízena datová schránka, sídlo a identifikační číslo osoby, bylo-li přiděleno,
h) název a sídlo organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, pro kterou byla zřízena datová schránka,
i) název orgánu veřejné moci, pro nějž byla zřízena datová schránka, sídlo a identifikační číslo osoby, bylo-li přiděleno,
…..
l) elektronická adresa nebo obdobný údaj pro vyrozumění o dodání datové zprávy do datové schránky,
m) datum a čas událostí spojených s provozem informačního systému datových schránek.

Přístup do datové schránky

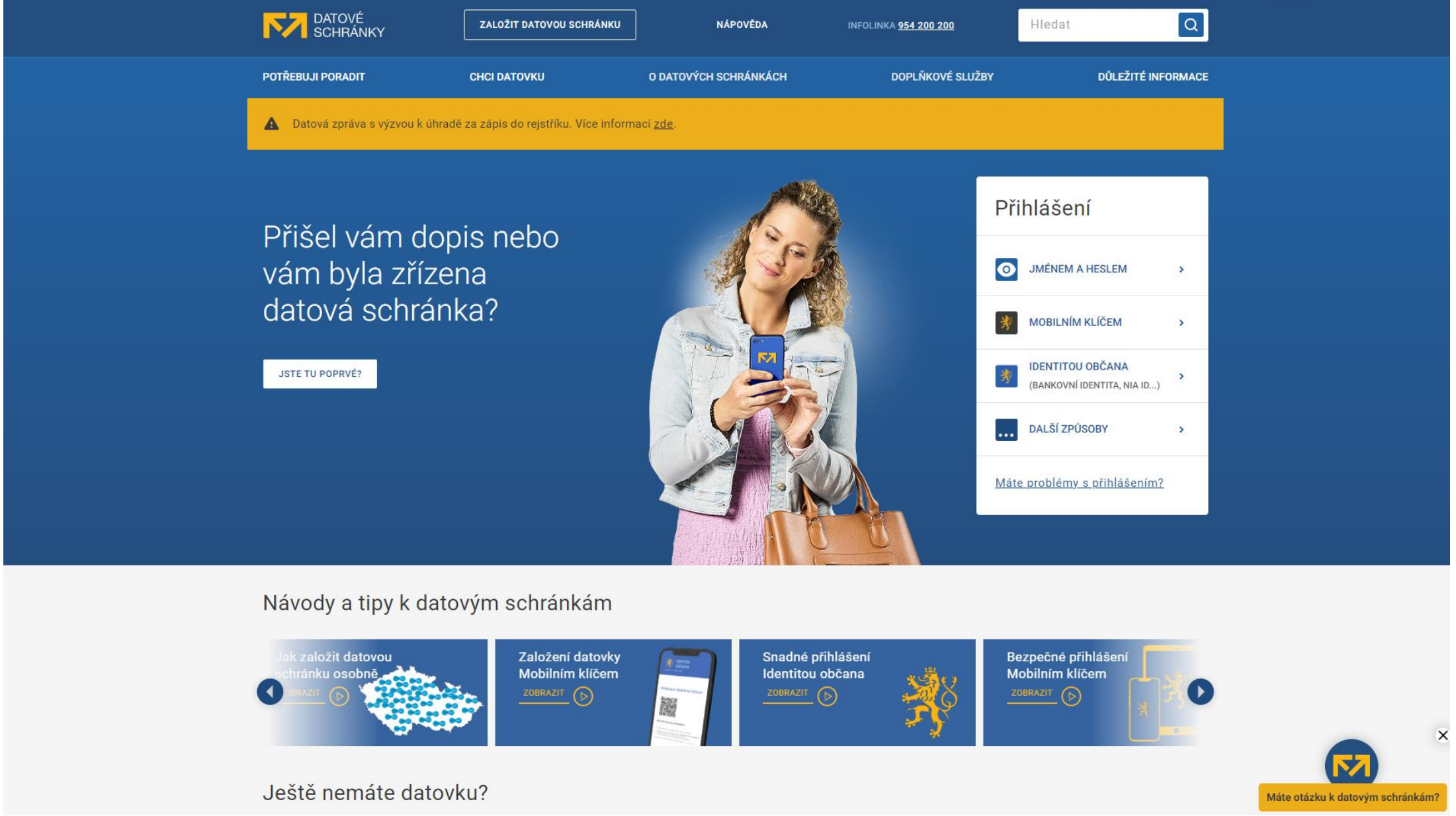
- Fyzická osoba
- Statutární orgán právnické osoby
- Vedoucí orgánu veřejné moci

- Dále
  - Pověřená osoba
  - Administrátor
  - Osoba oprávněná dle §18a

MUNI LAW

Archivace datových zpráv

- V datové schránce pouze po dobu 90 dnů
- Konvertovaná podoba
- Datový trezor - https://info.mojedatovaschranka.cz/info/cs/84.html
- … k zamyšlení: https://www.seznamzpravy.cz/clanek/ekonomika-finance-datova-schranka-archivace-90-dni-230346



https://info.mojedatovaschranka.cz/info/cs/

MUNI LAW

Autorizovaná konverze - § 22 ZoEU

- převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo datovém souboru, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky,

- převedení dokumentu obsaženého v datové zprávě do dokumentu v listinné podobě a ověření shody obsahu těchto dokumentů a připojení ověřovací doložky.

Subjekty provádějící konverzi

- Konverzi na žádost:
  - kontaktní místa veřejné správy
    - Pošty
    - Úřady
    - Notáři
  - advokáti
- Z moci úřední provádějí orgány veřejné moci pro výkon své působnosti.

Platnost konvertovaného dokumentu

- Do roku 2016: *Dokument, který provedením konverze vznikl (dále jen „výstup“), má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením výstup vznikl*
- **Od roku 2016: Dokument, který provedením konverze vznikl (dále jen „výstup“), má stejné právní účinky jako dokument, jehož převedením výstup vznikl (dále jen „vstup“).**
- Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy
- Přerazítkovávání časovým razítkem

MUNI LAW

Postup při konverzi § 24/1 ZoEU

a) ověří platnost kvalifikovaného elektronického časového razítka vstupu, je-li jím vstup opatřen,
b) ověří platnost uznávaného elektronického podpisu, je-li jím vstup podepsán, platnost uznávané elektronické pečetě, je-li jí vstup zapečetěn, nebo platnost uznávané elektronické značky, je-li jí vstup označen,
c) ověří integritu vstupu, je-li zajištěna jiným způsobem než podle písmene b) a lze-li tuto skutečnost ze vstupu zjistit a ověření provést.

Kdy nelze provést konverzi?

MUNI LAW

Konverze se neprovede pokud… (§ 24/4 ZoEU)

(4) Konverze se neprovádí

a) je-li dokument v jiné než v listinné podobě či v podobě datové zprávy,

b) jde-li o dokument v listinné podobě, jehož jedinečnost nelze konverzí nahradit, zejména o občanský průkaz, cestovní doklad, zbrojní průkaz, řidičský průkaz, vojenskou knížku, služební průkaz, průkaz o povolení k pobytu cizince, rybářský lístek, lovecký lístek nebo jiný průkaz, vkladní knížku, šek, směnku nebo jiný cenný papír, los, sázenku, geometrický plán, rys nebo technickou kresbu,

c) jsou-li v dokumentu v listinné podobě změny, doplňky, vsuvky nebo škrty, které by mohly zeslabit jeho věrohodnost,

d) není-li z dokumentu v listinné podobě patrné, zda se jedná o

1. prvopis,

2. vidimovaný dokument,

3. opis nebo kopii pořízenou ze spisu, nebo

4. stejnopis písemného vyhotovení rozhodnutí anebo výroku rozhodnutí vydaného podle jiného právního předpisu,

e) jde-li o dokument, který je výstupem, v jehož doložce je uveden údaj o tom, že vstup obsahuje viditelný prvek, který nelze plně přenést na výstup,

f) jde-li o vidimovaný dokument, v jehož ověřovací doložce je uveden údaj o tom, že dokument, ze kterého byl vidimovaný dokument pořízen, obsahoval viditelný zajišťovací prvek,

g) v případě provedení konverze na žádost, nebyl-li dokument obsažený v datové zprávě podepsán způsobem, se kterým jiný právní předpis spojuje při právním jednání vůči státu v souvislosti s výkonem jeho působnosti účinky vlastnoručního podpisu[11]), zapečetěn uznávanou elektronickou pečetí nebo označen uznávanou elektronickou značkou toho, kdo dokument vydal nebo vytvořil,

h) jde-li o dokument obsažený v datové zprávě, který nelze konvertovat do listinné podoby, například o zvukový nebo audiovizuální záznam,

i) pokud dokument nesplňuje technické náležitosti podle odstavce 3.

(5) Konverzí se nepotvrzuje správnost a pravdivost údajů obsažených ve vstupu a jejich soulad s právními předpisy.

MUNI LAW

Konverze advokáty

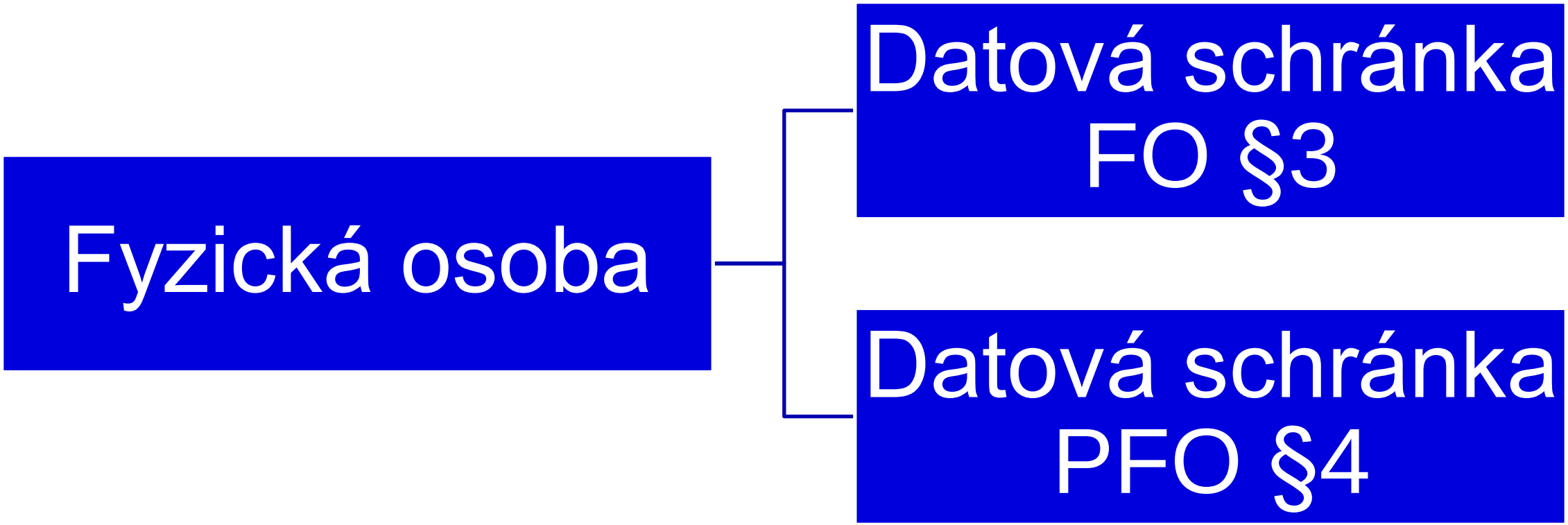
§ 23 ZoEU

- Konverzi na žádost provádějí kontaktní místa veřejné správy a advokáti za podmínek stanovených jiným právním předpisem

Zákon o advokacii

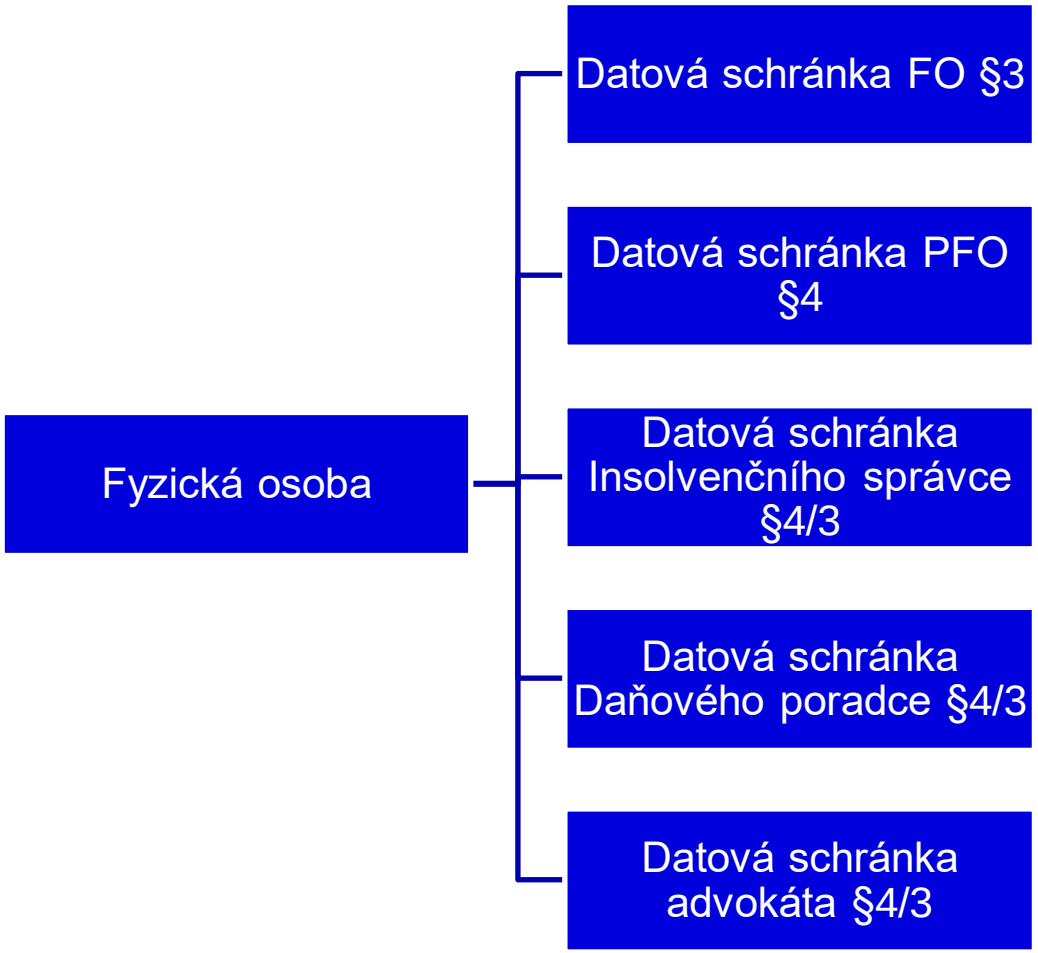
- V souvislosti s poskytováním právních služeb může advokát provádět autorizovanou konverzi dokumentů postupem podle zvláštního právního předpisu

Prolematika několika DS



MUNI LAW

Výjimka pro advokáty, insolvenční správce a daňové poradce



MUNI LAW

Judikatura obecně - elektronická kontraktace

30 Cdo 1230/2007 – Písemnost vs. elektronické nástroje

- Písemná forma právního úkonu předpokládá existenci dvou náležitostí, a to písemnosti a podpisu. Písemnost spočívá v tom, že projev vůle (právní úkon) jednajícího subjektu zahrnuje všechny podstatné náležitosti zachycené v písemném textu listiny. Písemný projev musí být zároveň podepsán, tj. je platný až po podpisu jednající osoby. Smlouva, která musí být písemná, avšak nebyla jejími účastníky podepsána, nemůže vyvolat zamýšlené právní následky.

33 Cdo 3210/2007

- Formulář vyplněný návštěvníkem webových stránek cestovní kanceláře je pouze impulzem k iniciativě cestovní kanceláře předložit zákazníkovi návrh cestovní smlouvy. Je-li tento návrh předkládán prostřednictvím elektronických prostředků, musí být opatřen zaručeným elektronickým podpisem; k platnému uzavření cestovní smlouvy je třeba, aby byl stejným způsobem akceptován.

Judikatura obecně - elektronická kontraktace

24 Co 696/2015

- Požadavku písemnosti ve smyslu § 561 odst. 1 o.z. je učiněno zadost i v situaci, kdy smluvní strana opatří smlouvu prostým elektronickým podpisem ve formě unikátního hesla či ID vázaného výhradně k její osobě, přičemž tak učiní mechanickými prostředky, tj. kliknutím na příslušné virtuální tlačítko. Takový podpis splňuje jak funkci identifikační, tak funkci autentizační.

Judikatura obecně - elektronická kontraktace

23 Cdo 3439/2018

- Rozhodčí doložka sjednána emailem byla uzavřena v písemné formě (posuzován český zákon, Newyorkská úmluva, modelové právo UNCITRAL)

Judikatura obecně - elektronická kontraktace

23 Cdo 3439/2018

- *„vznesla-li žalobkyně Námitky e-mailem […], který nebyl opatřen elektronickým podpisem, je závěr odvolacího soudu, že nedodržela písemnou formu Námitek, v souladu s judikaturou Nejvyššího soudu.“*
- Rozhodnutí je ale nutno kritizovat v souvislosti s tím, že soud se nijak nezabýval tím, co elektronický podpis je a zejména nezjišťoval, jestli žalovaná námitku neopatřila „prostým“ elektronickým podpisem. Už v tom případě by dané naplnilo podmínku podpisu. Rozhodnutí je tak nutno považovat za špatné a matoucí, je možno jej rovněž kritizovat i svým rigidním výkladem, kdy tímto rozhodnutím bylo *de facto* žalované následně upřeno právo na spravedlivý přístup k soudu.
- Soudy stále tápou (navíc toto rozhodnutí je velmi krátké)

Judikatura obecně podpis

Elektronický podpis a úřední ověření podpisu

KSPH 64 INS 26339/2015, 29 NSR 133/2017-B-36

- Nejvyšší soud zdůraznil, že úřední ověření je úzce vymezeným institutem, který je zákonem jasně definován.
- Soud dále poměrně vhodně rozvedl jednotlivé druhy podpisů, správně identifikoval, že zaručený elektronický podpis je jen předstupněm kvalifikovaného elektronického podpisu (rozebral poměrně kvalitně i dopady nařízení eIDAS, které upravuje problematiku elektronické identifikace)
- shrnul, že požadavek úředního ověření podpisu obecně vylučuje možnost využít elektronický podpis, jelikož chybí v českém právu takové zákonné propojení. To bylo ale explicitně zakotveno v určitou dobu IZ (nebo i jiné příklady viz výše).

X zákon o právu na digitální služby

Judikatura podpis

- **23 Cdo 3439/2018** – Rozhodčí doložka lze sjednat emailem
- **II. ÚS 3042/14** - Nutnost podepsat datovou zprávu odesílanou z datové schránky elektronickým podpisem (není třeba)
- **IV. ÚS 1829/13** – Nutnost podepsat přílohu datové zprávy (není třeba)
- **II – ÚS 3042/12** - K odeslání podání z emailu (uznávaně elektronicky podepsán) a jeho příloh (nepodepsány) – stačí jen podepsaný email
- **II. ÚS 289/15** - Nutnost elektronicky podepsat přílohu podání z datové schránky (není nutno)

Judikatura obecně - datová schránka

- **II ÚS 3518/11-1** – Rozhodný okamžik pro doručení datové zprávy (podání) soudu (a obecně jakémukoli veřejnému orgánu) – již doručením do příslušné DS
- **IV ÚS 2594/11** - Nelze se dovolávat nedoručení datové zprávy s odkazem na nedostatečné oprávnění osoby, která svým přístupem do datové schránky zapříčinila doručení datové zprávy
- **7 Afs 60/2015-32** - Nutnost primárně doručovat do datové schránky a až poté přistoupit k alternativním způsobům doručování
- **21 Cdo 5117/2014** - Doručení do sekundární datové schránky v rámci komunikace mezi orgány veřejné zprávy (nenastávají všechny účinky doručení – jen když dojde k otevření DS)
- **7 Asf 46/2010-51** – Zřízení více datových schránek (advokát, insolvenční správce, daňový poradce) – je to možné, záleží na „roli“ osoby
- **27 Cdo 143/2020** – Datová schránka identifikuje i v jiné roli (jednatel za družstvo, ale datová schránka jen jako FO - dostatečné)

Stanovisko Nejvyššího soudu Plsn 1/2015 (leden 2017)

- Elektronický nosič (příloha k datové zprávě) doprovázející samotnou datovou zprávu podanou prostřednictvím informačního systému datových schránek je považován za součást daného podání ve smyslu zákonné definice kladné na elektronické podání v občanském soudním řádu nebo v trestním řádu, ledaže z obsahu projevené vůle strany vyplývá něco jiného.
- Byl-li z datové schránky odesilatele (oprávněného) odeslán do datové schránky soudu elektronický dokument, který obsahuje podání ve věci samé, považuje se tento dokument (příloha) za řádně podepsaný (uznávaným elektronickým podpisem), i když samotný dokument elektronicky podepsán není. Pokud byl ale daný dokument odeslán z cizí datové schránky, musí být opatřen uznávaným elektronickým podpisem.
- V případě, že bylo podání v elektronické podobě podepsáno uznávaným elektronickým podpisem, nepoužije se tzv. fikce podpisu podle § 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů.

Stanovisko Nejvyššího soudu Plsn 1/2015 (leden 2017)

- Procesní úkon, učiněný prostřednictvím datové schránky se považuje za procesní úkon učiněný písemně a podepsaný osobou pro kterou byla datová schránka zřízena. Pokud je takovou osobou právnická osoba, má pak takový úkon učiněný prostřednictvím datové schránky stejnou účinnost, jako kdyby byl proveden osobou oprávněnou jednat za právnickou osobu.
- Soud primárně doručuje písemné vyhotovení rozhodnutí (či dalších písemností) do datové schránky v případě, že adresát má datovou schránku zřízenu. Pokud tomu tak není, přistoupí k jinému způsobu doručení. Soud pak rozhodnutí (či jiné písemnosti) doručuje prostřednictvím datové schránky jen jestli to povaha dané písemnosti umožňuje. Předpokladem ale je, že adresát má fyzickou osobu oprávněnou nebo pověřenou k přístupu do datové schránky a že nedošlo ke znepřístupnění datové schránky. Pokud právnická osoba prokáže, že neměla v době doručení osobu oprávněnou nebo pověřenou k přístupu do datové schránky (a daný stav nebyl zaviněn), nenastanou účinky doručení písemnosti.

Stanovisko Nejvyššího soudu Plsn 1/2015 (leden 2017)

- Má-li fyzická osoba zřízeno více datových schránek (např. datovou schránku fyzické osoby a zároveň datovou schránku podnikající fyzické osoby), je nutné písemnosti doručovat do té datové schránky, která odpovídá povaze doručované písemnosti. Účinky doručení nastanou ale rovněž doručením do nepříslušné datové schránky dané fyzické osoby s tím, že okamžik doručení nastává ve chvíli, kdy se do datové schránky přihlásí taková osoba, která má s ohledem na rozsah svého oprávnění přístup k dodaného dokumentu.
- Lhůta pro fikci doručení (10 dnů ode dne, kdy byl dokument dodán do datové schránky) se považuje za lhůtu procesní a její běh se počítá v občanském soudním řízení dle občanského soudního řádu a v trestním řízení dle trestního řádu.

CJEU - C-362/21

- 1) Článek 25 odst. 1 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES musí být vykládán v tom smyslu, že nebrání tomu, aby byl správní akt vyhotovený ve formě elektronického dokumentu prohlášen za neplatný, pokud je podepsán elektronickým podpisem, který nesplňuje požadavky tohoto nařízení k tomu, aby byl považován za „kvalifikovaný elektronický podpis“ ve smyslu čl. 3 bodu 12 tohoto nařízení, za podmínky, že neplatnost tohoto aktu není určena pouze z toho důvodu, že podpis na něm má elektronickou podobu.
- 2) Článek 3 bod 12 nařízení č. 910/2014 musí být vykládán v tom smyslu, že neexistence „kvalifikovaného certifikátu pro elektronický podpis“ ve smyslu čl. 3 bodu 15 tohoto nařízení postačuje k prokázání, že elektronický podpis nepředstavuje „kvalifikovaný elektronický podpis“ ve smyslu tohoto čl. 3 bodu 12, přičemž případná kvalifikace tohoto podpisu jako „profesionální elektronický podpis“ je v tomto ohledu irelevantní.
- 3) Nařízení č. 910/2014 musí být vykládáno v tom smyslu, že zápis elektronického podpisu v certifikátu vydaném poskytovatelem služeb vytvářejících důvěru nepostačuje k tomu, aby tento podpis splňoval požadavky stanovené tímto nařízením, aby mohl být považován za „kvalifikovaný elektronický podpis“ ve smyslu čl. 3 bodu 12 uvedeného nařízení. Pokud je taková kvalifikace zpochybněna v rámci soudního řízení, je vnitrostátní soud povinen ověřit, zda jsou splněny všechny kumulativní podmínky stanovené v uvedeném čl. 3 bodě 12, což vyžaduje, aby zejména ověřil, zda jsou splněny podmínky uvedené v článku 26 a příloze I téhož nařízení.

– 4) Článek 3 bod 12 a příloha I nařízení č. 910/2014 musí být vykládány v tom smyslu, že při kontrole souladu kvalifikovaného elektronického podpisu s požadavky uvedené přílohy nebrání okolnost, že jména podepisující osoby, která obvykle používá k jejich napsání cyrilici, byla transliterována do latinky, tomu, aby byl elektronický podpis této osoby považován za „kvalifikovaný elektronický podpis“ ve smyslu tohoto čl. 3 bodu 12, pokud je tento podpis jednoznačně spojen s podepisující osobou a umožňuje její identifikaci, což musí ověřit vnitrostátní soud.

MUNI LAW

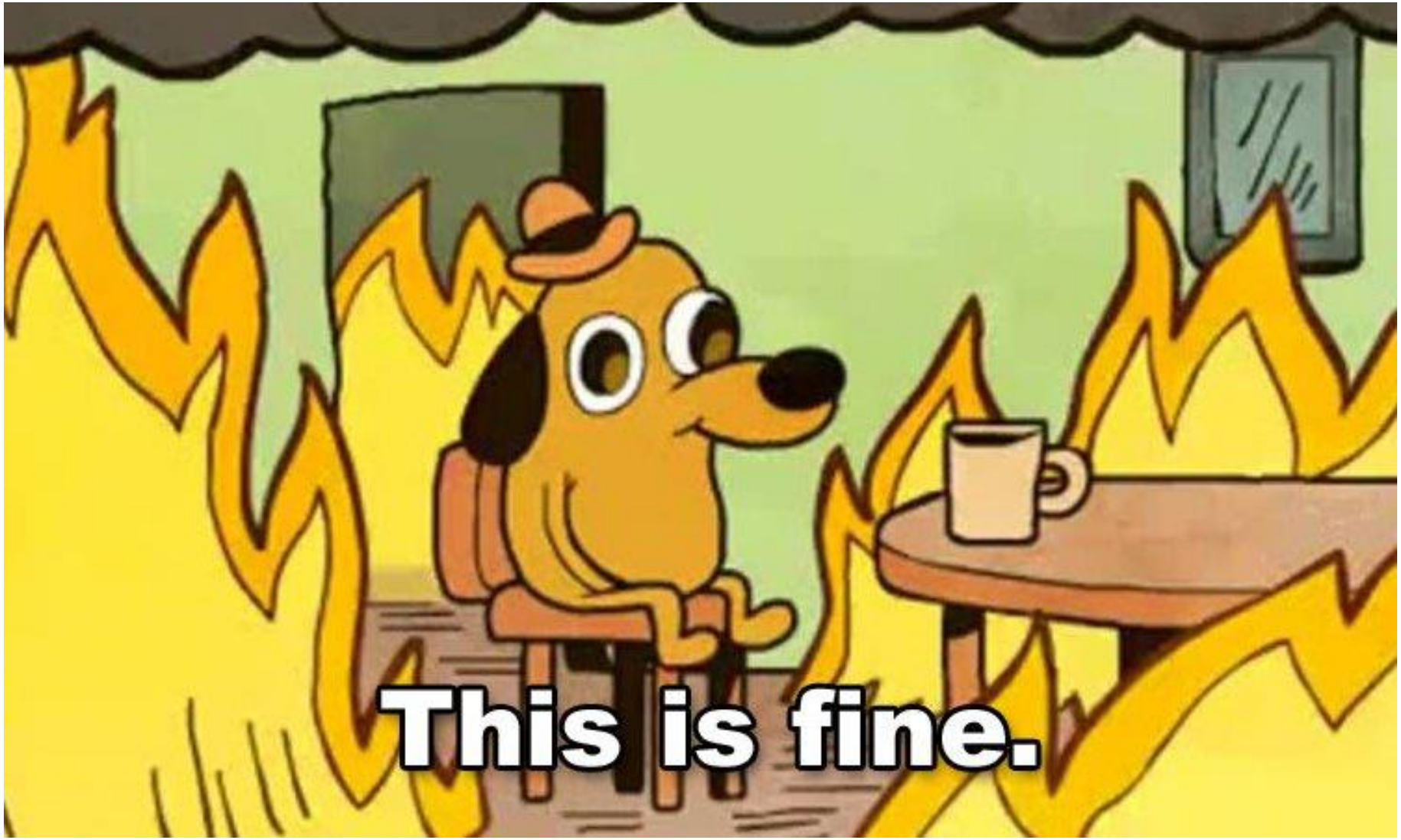
Postavení elektronického dokumentu

- **Rozsudek Nejvyššího správního soudu - 1 Afs 369/2020 – 54**
- Rozhodne-li se zákonodárce, že z rozumných důvodů je potřeba trvat na listinné podobě dokladů předkládaných při kontrole, může zpřísnit požadavky na formu dokumentů. V opačném případě je žádoucí zohlednit technologický i společenský pokrok. Právo je zapotřebí vykládat tak, aby reflektovalo potřeby ekonomické a společenské reality; nesmí tomu být naopak. Ekonomická a společenská realita nemá sloužit potřebám práva, jeho formalit a podřizovat se „přirozeným tendencím orgánů veřejné moci o maximální usnadnění rozhodovacího procesu“ (rozsudek Nejvyššího správního soudu ze dne 16. 4. 2008, č. j. 1 Ans 2/2008 - 52, č. 1626/2008 Sb. NSS). Lpění na listinné podobě dokumentů v situaci, kdy to není pro naplnění účelu právní úpravy nezbytné, je přepjatě formalistické.

Velmi zajímavé a smutné čtení

- https://www.epravo.cz/top/clanky/prosty-elektronicky-podpis-dle-eidas-v-soudni-praxi-114434.html

Závěrem?



MUNI
LAW

Děkuji za pozornost.

Nějaké otázky?

loutocky@muni.cz