Elektronické podpisy, úrovně záruky a právo na digitální služby

Jiří Peterka

Praha, 6.12.2019

1

co je největším problémem el. podpisů?

- jejich značně mezioborový charakter !!

lze vztáhnout na celou elektronizaci/digitalizaci

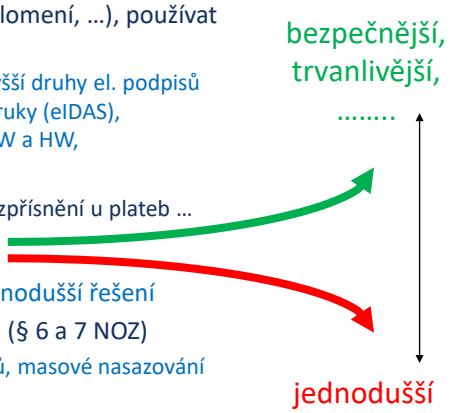
  - aby el. podpisy fungovaly, dalo se na ně spoléhat a mohly se v běžném životě používat, musí vzájemně spolupracovat lidé (nejméně) ze 3 oborů

  - problém: každý obor má svůj „pohled na svět“ (své priority, zájmy, terminologii, ..)
    - a již jen vzájemná domluva mezi lidmi z těchto oborů je ..... „složitá“
      - nehledě na osvětu !!
  - názor: právo některé aspekty elektronických podpisů nedoceňuje, jiné naopak přeceňuje
- srovnání:
  - v „kamenném světě“ (u listinných dokumentů a vlastnoručních podpisů) je situace odlišná: právo nepotřebuje další obory
    - výjimkou je písmoznalectví (pro zkoumání pravosti vlastnoručních podpisů)

2

problém divergence

- názor: různé obory reagují na současný trend (masové elektronizace / digitalizace) odlišně:
  - crypto a IT cítí potřebu posilovat spolehlivost a bezpečnost používaných řešení
    - vnímají (stále větší, automatizované) ohrožení a vývoj v čase, snaží se škálovat složitost (zneužití, prolomení, …), používat „časově odolná“ řešení
      - mají potřebu používat „silnější crypto“, vyšší druhy el. podpisů (kvalifikovaný, uznávaný), vyšší úrovně záruky (eIDAS), vícefaktorovou autentizaci, bezpečnější SW a HW,
      - pamatují na digitální kontinuitu …..
        - příklad: směrnice PSD2 od 14.9.2019 – zpřísnění u plateb …
  - právo (hlavně soukromé) hledá co nejjednodušší řešení
    - vychází z premisy, že lidé jednají čestně (§ 6 a 7 NOZ)
      - tendence k používání prostých el. podpisů, masové nasazování dynamických biometrických podpisů, ….
        - §7 zákona č. 297/2016 Sb: …. *lze použít jakýkoli druh el. podpisu …*

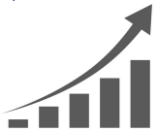


3

potřeba škálování a revokace

- pohled oborů IT a crypto:
  - „zlá protistrana“ má stále větší možnosti (automatizace útoků, působení na dálku, ….) a silnější nástroje (větší výpočetní sílu, znalosti, dovednosti, čas ….)
  - udržet „použitelnost“ dnešních řešení lze jen pomocí neustálého zvyšování nároků na to, co musí „zlá strana“ překonat, prolomit, napodobit, …..
    - s tím souvisí omezování v čase: platební karty jsou vydávány jen na omezenou dobu, stejně jako certifikáty, osobní doklady atd.
  - celkově je nutné používat řešení:

- se škálovatelnou složitostí
  - s možností zvyšovat (podle potřeby) složitost toho, co je nutné udělat pro prolomení, napodobení, zneužití
    - zvyšování výpočetní složitosti při vytváření padělků, kolizních dokumentů, ….



- s možností zneplatnění (revokace)
  - toho, co je soukromé / unikátní / charakteristické pro konkrétní osobu, a co nemá mít někdo jiný
    - aby se to již dále nedalo používat
  - příklady:
    - zneplatnění OP (osobních dokladů)
    - zablokování platební karty
    - revokace certifikátu

4

jak je na tom kryptografie?

- většina řešení v „elektronickém světě“ pro zajištění požadovaných vlastností využívá kryptografii
  - kryptografických algoritmů a technik je více, a lze je parametrizovat
    - například volbou velikosti klíčů a dalších parametrů
  - jinými slovy: kryptografie může mít různou „sílu“, kterou lze dále ovlivňovat
- důsledek: kryptografie je škálovatelná !
  - v okamžiku potřeby lze vždy nasadit „silnější“ kryptografii
  - bude to platit i po příchodu kvantových počítačů
    - existují i takové kryptografické algoritmy, které jsou vůči nim odolné

vlastnoruční podpis ani biometrika nejsou škálovatelné !

- asymetrická kryptografie umožňuje revokaci !
  - tj. kryptografie která pracuje se soukromým a veřejným klíčem
  - lze revokovat (předčasně ukončit platnost) certifikát, který byl vydán k soukromému klíči

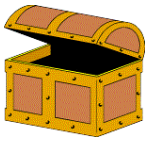
vlastnoruční podpis ani biometrika nejsou revokovatelné !

5

zastarávání kryptografických algoritmů

- konkrétní kryptografický algoritmus (s pevně danými parametry) vždy časem „zastará“
  - otázkou není „zda“, ale „kdy“

- jde o „zastarání“ ve smyslu oslabení a možnosti prolomení
  - konkrétní algoritmus (s pevně danými parametry) má vždy jen určitou „sílu“, a tím i výpočetní složitost, nutnou k jeho prolomení
    - takže je pouze otázkou času, kdy „zlá strana“ získá dostatečnou výpočetní sílu !
- příklad důsledků:
  - důvěrnost se zajišťuje šifrováním – ale to vydrží jen po omezenou dobu !!!
    - zašifrovaný obsah nelze „*nechat ležet*“ a doufat, že je chráněn navěky
      - algoritmus, použitý pro šifrování, po určité době zastará (oslabí) natolik, že „zlá strana“ dokáže obsah dešifrovat a seznámit se s ním
    - pozor zvláště u osobních údajů, biometriky atd.:
      - není radno je „dávat z ruky“ ani v zašifrované podobě
        - protože „*dříve či později se každý trezor otevře*“

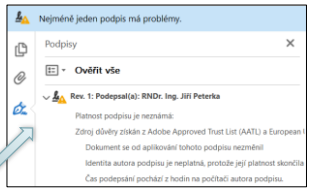


6

časová pojistka u elektronických podpisů

- zastarávání kryptografických algoritmů se netýká jen šifrování
  - ale také těch druhů elektronických podpisů, které jsou „kryptografické“
    - jde o kvalifikované, uznávané a zaručené elektronické podpisy
      - využívají asymetrickou kryptografii
- ale:
  - tyto druhy elektronických podpisů jsou chráněny proti zastarávání a oslabování kryptografických algoritmů - pomocí zabudované časové pojistky
    - časová pojistka způsobuje, že po určité době již není možné ověřit platnost elektronického podpisu
  - chrání to spoléhající se stranu před podvody
    - v době, kdy již lze vytvořit tzv. kolizní dokumenty
      - tj. takové, které jsou jiné, ale mají stejný podpis

Platnost od 31.07.2018 do 31.07.2019



příklad z roku 2017, ke stažení: https://www.earchiv.cz/down/koliznibalicek.zip

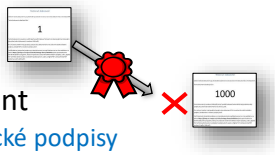
příklad kolize dle SHA 1

podpis „pasuje“ na oba (vzájemně kolizní) dokumenty a nelze již poznat, který byl skutečně podepsán

7

elektronické podpisy jsou nepřenosné

- dokud se neprojeví časová pojistka (dokud je možné ověřit podpis jako platný), lze se spoléhat na to, že el. podpis nejde přenést na jiný dokument
  - platí to pro kvalifikované, uznávané a zaručené elektronické podpisy



- připomenutí:
  - tyto druhy el. podpisů vznikají „semletím“ soukromého klíče a podepisovaného dokumentu
    - jsou tedy závislé na tom, co je podepsáno… nelze je vytvořit dopředu

- jinými slovy:
  - u těchto druhů podpisů je jejich vazba na podepsaný dokument pevně daná

výpočtem

- srovnání:
  - je to podobné jako u vlastnoručních podpisů na listinných dokumentech
    - kde dostatečně pevná vazba vzniká vsáknutím inkoustu do papíru

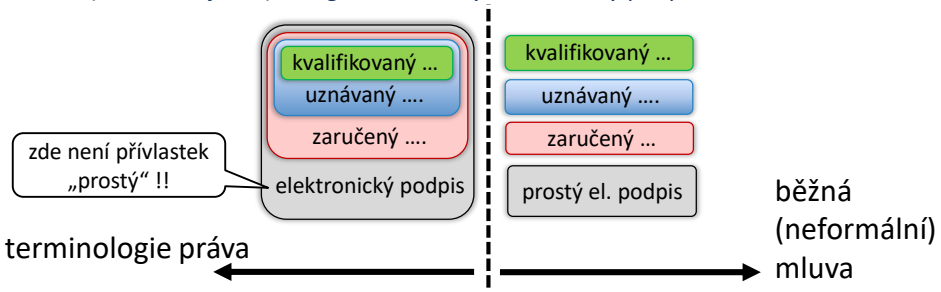
- ale: kvalifikované, uznávané a zaručené el. podpisy dokáží chránit podepsaný dokument proti jakékoli změně
  - což vlastnoruční podpisy nedokáží !!

jde o tzv. zajištění integrity (eIDAS, čl. 26 písm. d)

8

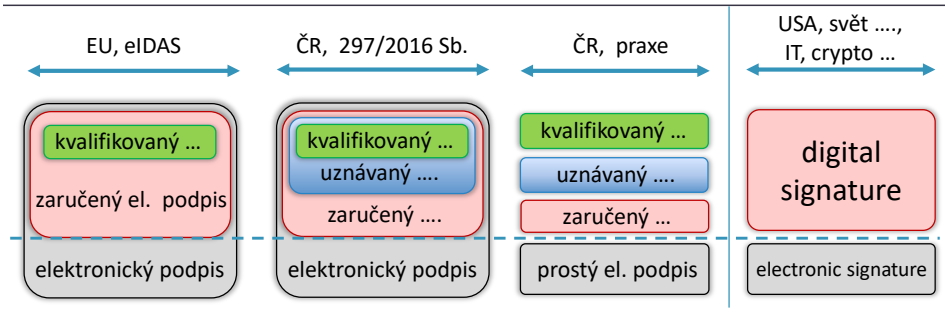
co jsou prosté elektronické podpisy?

- možné odpovědi:
  - právně neexistují – nejsou pojmem zákona (právní předpisy o nich nehovoří)
    - jde pouze o neformální označení
  - jsou *„tím, co zbyde, když rezignujeme na všechny dosud vyjmenované (a další) vlastnosti a přínosy elektronických podpisů“*
    - neboli: když po nich nebudeme nic požadovat, ale také od nich nebudeme nic očekávat
  - jsou zbytkovou kategorií
    - když vezmeme (největší) kategorii *„elektronický podpis“* a odečteme od ní (druhou největší) kategorii *„zaručený elektronický podpis“*



9

srovnání s EU a s USA

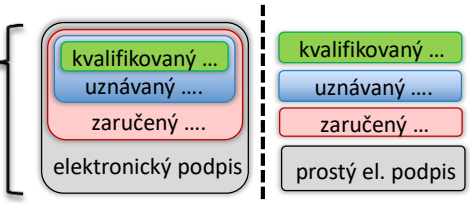


- v USA (a často i jinde, též v odborné literatuře, ...)
  - k rozlišení stačí 1 přívlastek:
    - **digital signature**: podpis je „počítaný“ (vznikající výpočtem, „z 0 a 1“)
      - využívá kryptografii (matematiku) a její algoritmy a metody ...
    - **electronic signature**: podpis není „počítaný“, vzniká jinak než výpočtem
      - např. naskenováním křivky vlastnoručního podpisu, napsáním nějakého textu, ...
- v ČR/EU
  - k rozlišení potřebujeme 2. přívlastek (navíc k přívlastku „elektronický“)
    - a ještě si musíme pomáhat zavedením neformálního přívlastku „prostý“ .....

10

ad prosté elektronické podpisy

- důsledek:
  - když někdo říká *„má tam být elektronický podpis“*, neznamená to *„má tam být prostý elektronický podpis“*
    - viz např. rozhodnutí NS 26 Cdo 1230/2019:
      - *„bylo nutné e-mail …. doplnit o elektronický podpis“*
  - říká, že tam má být →



  - měl by ale říci konkrétněji:
    - jaký druh elektronického podpisu požaduje – a to v závislosti na tom, co od něj očekává, co by měl splňovat ……
      - zda stačí prostý elektronický podpis, nebo
      - zda stačí zaručený elektronický podpis (který nezaručuje identitu podepsané osoby)
      - nebo zda stačí uznávaný elektronický podpis
        - tj. zaručený elektronický podpis, založený na kvalifikovaném certifikátu
      - nebo zda je nutný kvalifikovaný elektronický podpis

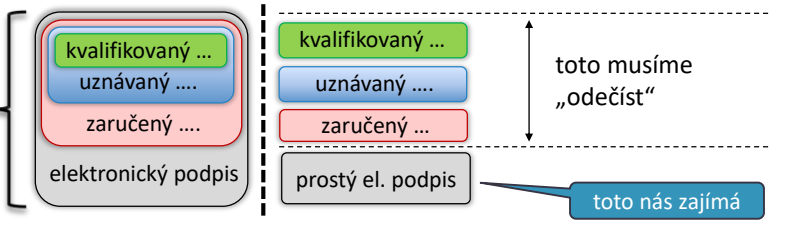
11

co všechno může být prostým el. podpisem?

- obecně: cokoli, co „je z nul a jedniček“ ´(co je elektronické)
  - ale nesplňuje to požadavky, kladené na zaručené elektronické podpisy !
- připomenutí:

pozor: to není definice prostého el. podpisu, ale „všech druhů“ el. podpisů

„elektronickým podpisem“ [*se rozumí*] 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;



- přirovnání:
  - je to jako kdybychom (v listinném světě) od podpisů odečetli vlastnoruční podpisy
    - co nám potom zbyde?

elektronických podpisů — zaručené el. podpisy

12

co všechno může být prostým el. podpisem?

- prosté elektronické podpisy nejsou v nařízení eIDAS explicitně řešeny
  - nařízení nechce říkat a neříká, jak mají „vypadat“
    - viz např. *„Komise může prostřednictvím prováděcích aktů určit referenční čísla norem pro zaručené elektronické podpisy …..“*
      - také technické normy a standardy se zabývají až zaručenými el. podpisy
  - ani jak se mají používat (ve „veřejných službách“ !)
    - viz např. *„Pokud členský stát … požaduje zaručený elektronický podpis, uznává zaručené elektronické podpisy ….“*

to říká až pro zaručené el. podpisy

to říká až pro zaručené el. podpisy

- jediné ustanovení, kde jsou „prosté“ el. podpisy již zahrnuty, je v čl. 25
  - *„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“.*
- otázka:
  - jak tomu rozumět?
    - názor: jde o „ubírání“ (viz: upírání) právních účinků, nikoli o jejich „přidávání“
      - a prosté el. podpisy z nařízení eIDAS žádné účinky nemají

názor: může být použito (a nesmí být odmítnuto) například tam, kde by v listinné podobě stačil nepodepsaný či pouze parafovaný dokument, či podpis nahrazený mech. prostředky

13

prosté el. podpisy v zákoně č. 297/2016 Sb.

- prosté elektronické podpisy jsou (nepřímo) řešeny až v naší národní legislativě
  - v „adaptačním“ zákoně č. 297/2016 Sb., o službách vytvářejících důvěru
    - fakticky pro „soukromoprávní jednání“
      - nikoli „směrem k OVM“ (§ 6 odst. 1) či „od OVM“ (§ 5)

§ 7 : 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 nebo § 6 odst. 1.

- otázka:
  - jaké jsou účinky takovéhoto podepsání?

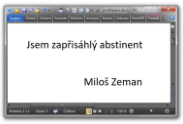
zaručují integritu (neměnnost) podepsaného dokumentu

- připomenutí: různé druhy el. podpisů mají různé vlastnosti
  - kvalifikované a uznávané el. podpisy zaručují identitu podepsané osoby
  - zaručené el. podpisy nemusí zaručovat identitu podepsané osoby
  - prosté elektronické podpisy nezaručují nic

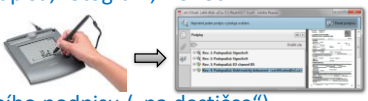
14

co bývá v praxi prezentováno jako prostý el. podpis?

- příklady:
  - napsaný či nakreslený podpis
    - text, napsaný do dokumentu (pomocí editoru)
    - křivka, nakreslená do dokumentu (programem/editorem)
      - někdy nahrazeno „rukopisným fontem“



  - obrázkový podpis
    - do dokumentu je vložen obrázek
      - např. s naskenovanou křivkou vlastnoručního podpisu, fotografií, ikonou ….
  - biometrický podpis
    - do dokumentu jsou vložena biometrická data
      - nejčastěji digitálně nasnímaná křivka vlastnoručního podpisu („na destičce“)
        - ale mohou to být i jiná biometrická data – např. otisk prstu, vzorek sítnice, ….
    - varianta: dynamický biometrický podpis
      - při digitálním snímání vlastnoručního podpisu je kromě křivky snímána i dynamika podepisování (rychlost, přítlak)
  - ……



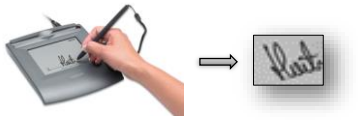
- vždy jde o nějaký vzorek, který je/měl by být (v různé míře) unikátní a charakteristický pro konkrétní osobu

15

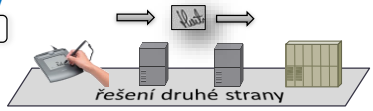
příklad: dynamický biometrický podpis

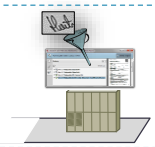
- časová posloupnost dějů:
  - T1: zákazník odevzdává vzorek svého vlastnoručního podpisu na destičce
    - vzorek jeho podpisu (biometrika) existuje sám o sobě
  - T2: odebraný vzorek prochází interními systémy druhé strany
    - vzorek je nadále pod výhradní kontrolou druhé strany
      - zatímco klient nad ním již nemá žádnou kontrolu
  - T3: odebraný vzorek je vkládán do dokumentu
    - křivka podpisu v nezašifrované (viditelné) podobě, další ev. biometrika obvykle již zašifrovaná
  - T4: druhá strana podepisuje (pečetí) dokument
    - používá „kryptografický“ podpis/pečeť
      - tím „fixuje“ dokument i s vloženým obsahem (zajištění integrity)

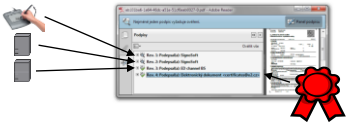
je vlastně „dvoustranný“



jak je to s jejich certifikací? eIDAS je neřeší ….







16

prosté vs. „kryptografické“ el. podpisy

- „kryptografické“ el. podpisy (kvalifikované, uznávané a zaručené)
  - neexistují samy o sobě
    - protože jsou závislé na tom, co je podepisováno
  - nelze je vytvořit dopředu
    - dokud nevíme, co bude podepisováno
  - jsou nepřenosné
    - jejich vazba na podepisovaný dokument je pevně dána
  - podepisující osoba rozhoduje o tom, co podepisuje
    - nelze podepsat „něco jiného“
  - je zřejmé co je „aktem podepsání“
    - spuštění výpočtu podpisu
- prosté el. podpisy (obrázkové, biometrické, dynamické biometrické)
  - mohou existovat samy o sobě
    - např. obrázek (sken vlastnoručního podpisu), biometrika (digitálně nasnímaný vlastnoruční podpis), ….
  - lze je vytvořit dopředu
    - ještě nemusí být známo, co bude podepsáno
  - jsou přenosné
    - jejich vazba na podepisovaný dokumentu není pevně dána
    - někdo musí tuto vazbu vytvořit !!
      - biometrické podpisy: vazbu vytváří druhá smluvní strana, nikoli podepisující
  - co je „aktem podepsání“?
    - vytvoření vzorku, nebo vazby?

17

rozdíl v nakládání s tajemstvím

- další významná odlišnost:
  - týká se *„toho, co je pro podepisující osobu unikátní a charakteristické“* (její tajemství), a čím by neměl disponovat (co by neměl mít/znát) nikdo jiný
- „kryptografické“ el. podpisy
  - tj. kvalifikované, uznávané a zaručené
  - onou unikátní charakteristikou (tajemstvím) je soukromý klíč 
  - platí, že:
    - unikátní charakteristika není součástí výsledného podpisu / dokumentu
      - soukromý klíč nemusí podepisující osoba „dávat z ruky“
  - soukromý klíč není zastaráváním kryptografických algoritmů ohrožen
    - ohrožena je záměna podepsaných dokumentů
      - a před tou chrání časová pojistka !!!
  - samotný podpis nepotřebuje důvěrnost
    - není nutné ho chránit, může být veřejný
    - „do časové pojistky“ není přenosný
- prosté el. podpisy
  - psané, obrázkové, biometrické, …
  - onou unikátní charakteristikou (tajemstvím) je přímo samotný podpis
    - vlastně: vzorek fyzické osoby 
  - platí, že:
    - unikátní charakteristika (vzorek) je součástí výsledného dokumentu
  - otázka důvěrnosti podpisu/vzorku:
    - psané podpisy: není co chránit
    - obrázkové podpisy: nejsou chráněny
      - lze je snadno použít jinde
    - biometrické podpisy: obvykle jsou chráněny šifrováním 
      - může vytvářet i vazbu na dokument
      - ale to vydrží jen omezenou dobu !!!!
        - je ohroženo zastaráváním algoritmů

18

další rozdíly

- „kryptografické“ el. podpisy
  - tj. kvalifikované, uznávané a zaručené
  - lze je revokovat ⟷ nelze je revokovat
    - přesněji: lze revokovat certifikát, vydaný k soukromému klíči
      - tj. případná kompromitace „tajemství“ má řešení
    - není co revokovat/zneplatnit
      - tj. případná kompromitace „tajemství“ nemá řešení
  - jsou škálovatelné ⟷ nejsou škálovatelné
    - lze používat různě „silné“ kryptografické algoritmy
    - nelze používat různě „silné“ charakteristiky téže osoby
  - chrání je „časová pojistka“ ⟷ nemají žádnou „časovou pojistku“
  - mohou být „časově odolné“ ⟷ nejsou „časově odolné“
    - lze udržovat jejich digitální kontinuitu
      - udržovat je v takovém stavu, aby i po delší době bylo možné spolehlivě ověřit platnost jejich podpisů/pečetí
        - existují na to technické normy
        - počítá s tím čl. 34 nařízení eIDAS
    - výjimka: u (dynamických) biometrických podpisů lze udržovat digitální kontinuitu u podpisu/pečeti druhé smluvní strany
- prosté el. podpisy
  - psané, obrázkové, biometrické, …

19

nově navrhované koncepty

- návrh zákona o právu na digitální služby (PSP: tisk č. 447) přichází s novými koncepty elektronického podepisování (ve svém § 6)
  - **legalizace el. podpisu**
    - představa: jde o překlopení procesu legalizace z listinného světa do elektronického světa
      - se svým elektronickým dokumentem „zajdu za někým“, kdo ověří můj (elektronický) podpis
        - může to být člověk
        - může to být stroj
          - informační systém veřejné správy, ke kterému se musím přihlásit s úrovní záruky „vysoká“
  - důsledek:
    - takto „legalizovaný“ el. podpis pak může nahradit úředně ověřený podpis
      - ale také uznávaný el. podpis
  - **„zapsání kvalifikovaného certifikátu“**
    - jde o řešení problému s jednoznačnou identifikací držitele kvalifikovaného certifikátu
      - je tam povinně jen jméno (Jan Novák)
        - ale osob stejného jména může být více – o kterého z nich jde?
    - představa: držitel sám nechá zapsat údaje o svém certifikátu do základního registru obyvatel
      - díky tomu si spoléhající se osoba (z veřejné správy) bude moci zjistit, o koho konkrétně jde
  - důsledek:
    - uznávaný elektronický podpis pak může nahradit úředně ověřený podpis

20

konkrétní navrhované znění

§ 6

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) 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.

21

úrovně záruky (eIDAS)

- otázka:
  - lze nějak jednoduše ohodnotit míru spolehlivosti/důvěryhodnosti/pravosti/jistoty při jednání v elektronické podobě?

například při „legalizaci“ el. podpisu?

- odpověď: je to možné
  - díky nařízení eIDAS, které zavádí tzv. **úrovně záruky** (LoA, Level of Assurance)

úroveň záruky	příklad z praxe	požadavky	cíl (…. riziko zneužití nebo změny totožnosti)
Vysoká (High)	nová eOP 	nutný HW (čipová karta/token)	předejít ….
Značná (Substantial)	„jméno, heslo, SMS“, bankovní identita, ….	nutná 2-faktorová autentizace	značně snížit ….
Nízká (Low)	přihlašování k ISDS	stačí 1-faktorová autentizace	snížit ….
…… (nulová)	jméno a heslo	stačí 1- faktorová autentizace	…..

22

„zasazení“ úrovní záruky do práva

- obecně:
  - úroveň záruky je vztahována k prostředku pro elektronickou identifikaci
    - dle zákona č. 250/2017 Sb. o elektronické identifikaci
- zjednodušeně:
  - prostředkem pro elektronickou identifikaci je *„to co používáme pro přihlašování“*:
    - nová elektronická eOP …. úroveň vysoká
    - prostředek *„Jméno, heslo a SMS“* …. úroveň značná
      - potenciálně též:
        - jiná kombinace jména, hesla a OTP (One Time Password, jednorázové heslo),
        - jméno, heslo, certifikát (může být i „soft“)
        - jméno, heslo, „mobilní klíč“
        - ……..
    - jméno a (opakovaně použitelné) heslo … úroveň nízká
- princip využití:
  - právní předpisy pro konkrétní úkon/jednání/přístup/využití služby stanoví požadovanou (minimální) úroveň záruky

23

konkrétní příklady

- zákon o právu na digitální služby (t.č. v návrhu)
  - počítá se vznikem katalogu služeb
    - u každé služby by měla být stanovena úroveň záruky, požadovaná pro její využití
    - default (*„pokud to nebude stanoveno“*) bude úroveň **„značná“**

§ 12, Právo na elektronickou identifikaci a autentizaci
Není-li v katalogu služeb pro využití digitální služby stanovena úroveň záruky prostředku pro elektronickou identifikaci, uživatel služby má právo provést svou identifikaci a autentizaci prostředkem pro elektronickou identifikaci podle své volby nejméně v úrovni značná.

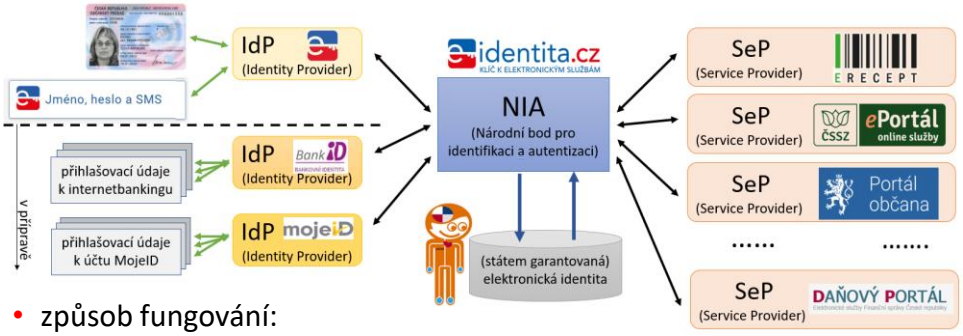
  - počítá s možností náhrady úředně ověřeného podpisu nebo uznávaného elektronického podpisu (viz dříve)
    - též „strojově“ – skrze záznam od ISVS, ke kterému se uživatel přihlásil prostředkem s úrovní záruky **„vysoká“**
- zákon č. 300/2008 Sb. o el. úkonech a autorizované konverzi

§ 27, Společná, přechodná a závěrečná ustanovení
§2, 3, 4, 6: Úředně ověřený podpis žádosti …. se nevyžaduje, je-li žádost podána …. prostřednictvím informačního systému datových schránek **s využitím přístupu s vysokou úrovní záruky.**

24

příklad využití úrovní záruky - NIA

- v ČR jsme si pro přihlašování ke službám eGov zvolili nepřímý model
  - NIA (Národní bod pro identifikaci a autentizaci) je prostředníkem mezi:
    - poskytovateli identity (IdP, Identity Provider) a poskytovateli služeb (SeP, Service Provider)

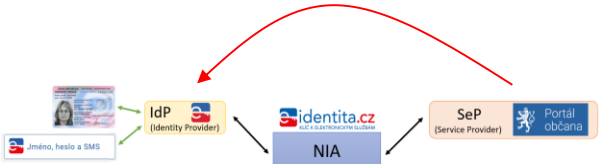


- způsob fungování:
  - zájemce (uživatel) chce využívat nějakou službu – jde za konkrétním SeP
  - SeP „pošle“ zájemce za NIA (a té sdělí svůj požadavek na úroveň záruky)
    - vysoká, značná, nízká
  - NIA nabídne zájemci jen ty IdP, kteří umožňují přihlášení s požadovanou úrovní záruky
  - zájemce si vybere jednoho IdP a ten mu nabídne jen takové možnosti přihlášení, které mají požadovanou úroveň záruky

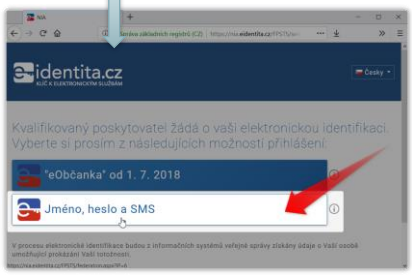
25

jak to funguje v praxi?

- příklad: přihlášení k Portálu občana (https://obcan.portal.gov.cz]



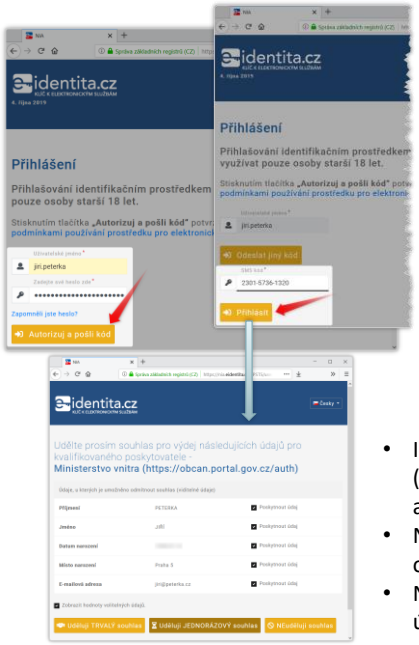
uživatel si vybere, přes koho se chce přihlásit
(přes kterého IdP, resp. přes který systém el. identifikace)



IdP (systém el. identifikace) nabízí více možností přihlášení (možnost použití více prostředků el. identifikace). Uživatel si mezi nimi vybírá ….

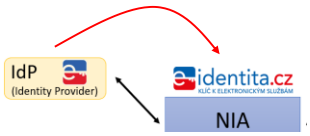
26

jak to funguje v praxi?



uživatel se vůči zvolenému IdP (poskytovateli el. identifikace):

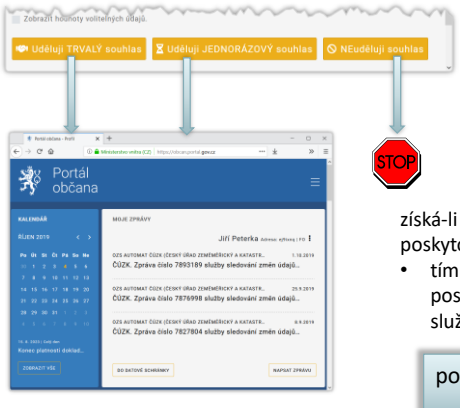
- identifikuje (uživatelským jménem)
- autentizuje (heslem a SMS kódem)

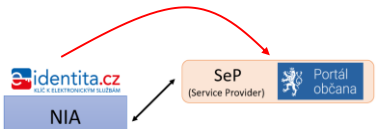


- IdP (poskytovatel el. identifikace) vrací do NIA (národního bodu) potvrzení, že uživatel se řádně autentizoval
- NIA získává ze základních registrů požadované údaje o uživateli
- NIA žádá uživatele o souhlas s poskytnutím jeho údajů zvolenému poskytovateli služby (SeP)

27

jak to funguje v praxi?





získá-li NIA (národní bod) souhlas uživatele, předává údaje poskytovateli služby (SeP)

- tím je dokončeno přihlášení (ke službě zvoleného poskytovatele služeb) a uživatel může začít využívat službu .....

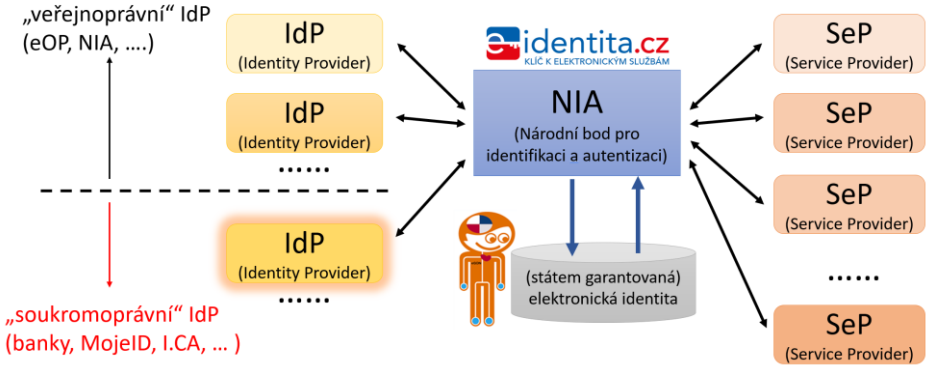
poskytovatelem služby (SeP) v ČR dnes může být jen orgán veřejné moci !!!

- výhody nepřímého modelu:
  - poskytovatelé služeb (SeP) se nemusí přizpůsobovat různým poskytovatelům identity (IdP)
    - protože s nimi nekomunikují (komunikují jen s prostředníkem)
  - poskytovatelé identity (IdP) se nemusí přizpůsobovat poskytovatelům služeb …
- (ne)výhody nepřímého modelu:
  - vše stojí a padá s prostředníkem (NIA, národní bod), prostředník „ví o všem“
  - národní bod (SZR, resp. stát) rozhoduje o tom, kdo smí fungovat jako SeP i jako IdP

28

jak to (teprve) bude fungovat v praxi?

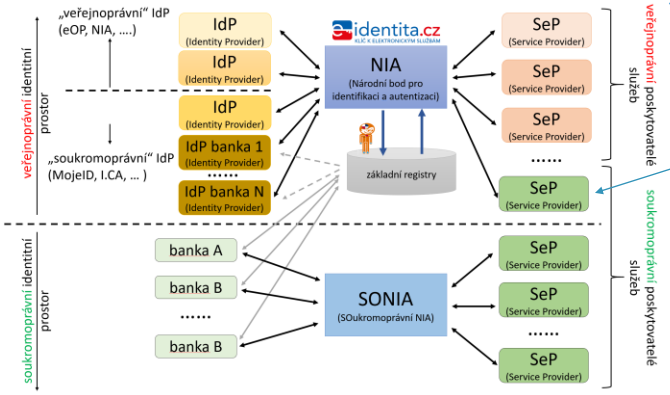
- poskytovatelem identity (IdP) může být i soukromoprávní subjekt
  - některé subjekty již deklarovaly zájem, konkrétně:
    - banky: tzv. „bankovní identita“ - zřejmě aspirují na úroveň „značná“
      - ale musí být nejprve upravena bankovní legislativa (již „v procesu“)
    - I.CA (čipová karta Starcos), MojeID (token FIDO2) – zřejmě aspirují na úroveň „vysoká“



29

projekt SONIA

- SONIA, od: „SOukromoprávní NIA“
  - jde o společný projekt bank (České bankovní asociace)
  - záměrem je vytvořit jakýsi paralelní „národní bod“
    - který by mohl zprostředkovávat identitní služby jakýmkoli SeP
      - hlavně těm soukromoprávním (např. eshopy, pojišťovny, utility, operátoři, banky, ...)



- „veřejnoprávní“ NIA poskytuje své služby jen veřejnoprávním SeP
  - do budoucna může poskytovat služby jen některým soukromoprávním SeP
    - takovým, které mají ze zákona povinnost ověřovat totožnost
      - a to lze od 1.7.2020 jen přes tzv. kvalifikovaný systém el. identifikace, dle zákona č. 250/2017 Sb.

30

podrobněji k úrovním záruky

- pro určení celkové úrovně záruky se rozlišují 3 různé fáze/etapy:

nízká, značná, vysoká

1. fáze „počátečního zavedení do systému“
   - vytvoření uživatelského účtu,
   - získání údajů o žadateli a jejich ověření
   - přidělení/vygenerování přístupových údajů
   - ….

   Enrollment
   přihlášení
   provádí se 1x
   dle nařízení EK 2015/1502

2. fáze správy přístupových (a dalších) údajů
   - předání/doručení přístupových údajů
   - zneplatnění kompromitovaných přístupových údajů
   - vydání nových přístupových údajů
   - aktualizace údajů o uživateli v rámci jeho účtu
   - …..

   Electronic identification means management
   správa prostředků pro elektronickou identifikaci
   může se opakovat (občas, podle potřeby)

3. fáze rutinního používání
   - vlastní používání přístupových údajů
     - přístup/přihlašování ke službě a její využívání

   Authentication
   autentizace
   opakuje se často (rutinně)

31

podrobněji k úrovním záruky

- představují celkové hodnocení (dané hlavně nejslabším článkem) přes všechny fáze a jejich dílčí části/faktory
- úroveň záruky vysoká:
  - identita musí být spolehlivě zjištěna a ověřena vůči autoritativnímu zdroji
    - oproti ROB /ISEO ……, pravost osobních dokladů musí být ověřena, ….
  - pro přihlašování (autentizaci) se vyžaduje nejméně 2-faktorová autentizace
    - jedním z faktorů musí být certifikát, uložený v čipové kartě / USB tokenu
      - musí to být tzv. „hard“ certifikát – není možné ho z čipové karty/tokenu dostat ven
  - prostředek pro elektronickou identifikaci (karta/token) je předán výhradně adresátovi
    - a je ověřeno, že jej převzal skutečně (výhradně) adresát
      - prakticky to znamená: je nutné fyzické **předání „z ruky do ruky“**
  - existují mechanismy pro zneplatnění (revokaci) certifikátu/prostředku …..
    - a vydání nových prostředků
- úroveň záruky značná:
  - ověřování identity je o něco méně přísné
    - důvěřuje se (úředním) osobním dokladům, kontroluje se jejich pravost a platnost, …..
  - předání přístupových údajů (prostředků ….) nemusí nutně být „z ruky do ruky“
  - pro autentizaci se nevyžaduje „hard“ certifikát (v bezpečném prostředku)
    - ale stačí i „soft“ certifikát. Lze použít i jednorázová hesla (OTP, One Time Password)

32