

MVŠO

MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUČ



VYSOKÉ UČENÍ
TECHNICKÉ
V BRNĚ

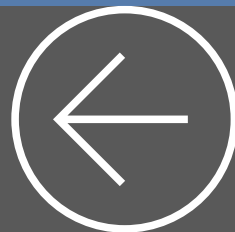
Dynamický biometrický podpis a nařízení GDPR

Prof. Ing. **Vladimír Smejkal**, CSc., LL.M.

Moravská vysoká škola Olomouc, o.p.s.

Vysoké učení technické v Brně, Fakulta podnikatelská

vladimir.smejkal@mvso.cz
www.mvso.cz | www.znalci.cz



Co to je dynamický biometrický podpis



Dynamický biometrický podpis (DBP)

- Alternativa ke kryptografickému elektronickému podpisu.
- Vlastnoruční podpis doplněný technologickým „backgroundem“ zajišťuje vysokou bezpečnost při zachování klasického způsobu podepisování.
- Uživatelsky daleko přijatelnější varianta oproti používání certifikátů (časově limitovaná platnost certifikátů a otravná práce s nimi).



Princip vytvoření DBP

- Snímá se vlastnoruční podpis na digitalizačním tabletu, vytvořený buď jakýmkoliv nástrojem nebo speciálním perem.
- Data obsahují 1. obrázek (statický podpis), 2. dynamické vlastnosti podpisu spojeného s typickým chováním podepisující se osoby.

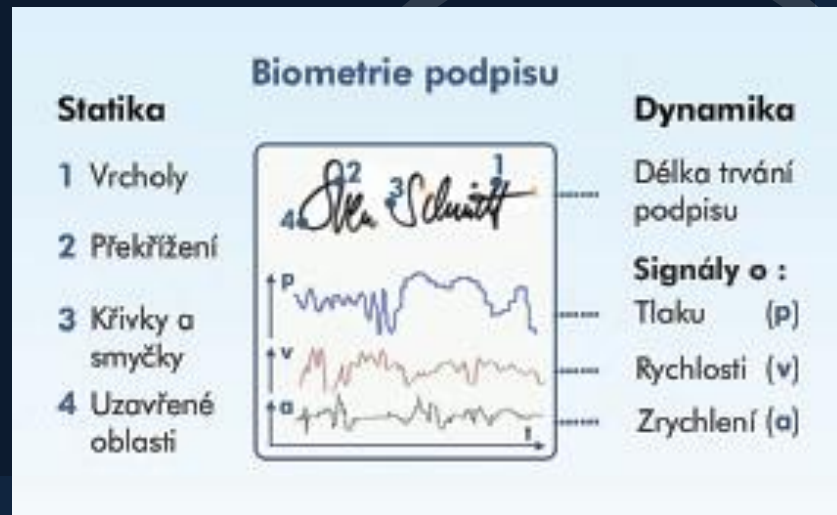


Princip vytvoření DBP

DBP obsahuje informace o tom:

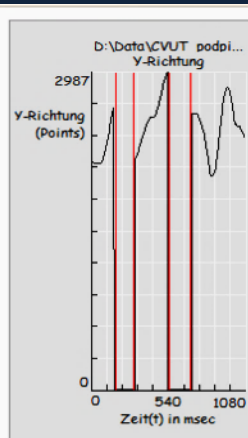
- jak podpis byl vytvořen,
- jaké jsou charakteristické znaky podepisující se osoby, její návyky a projevy chování.

Tyto vlastnosti představují biometrickou stopu, která je unikátní pro každého jednotlivce a nemůže být padělatelem reprodukována.

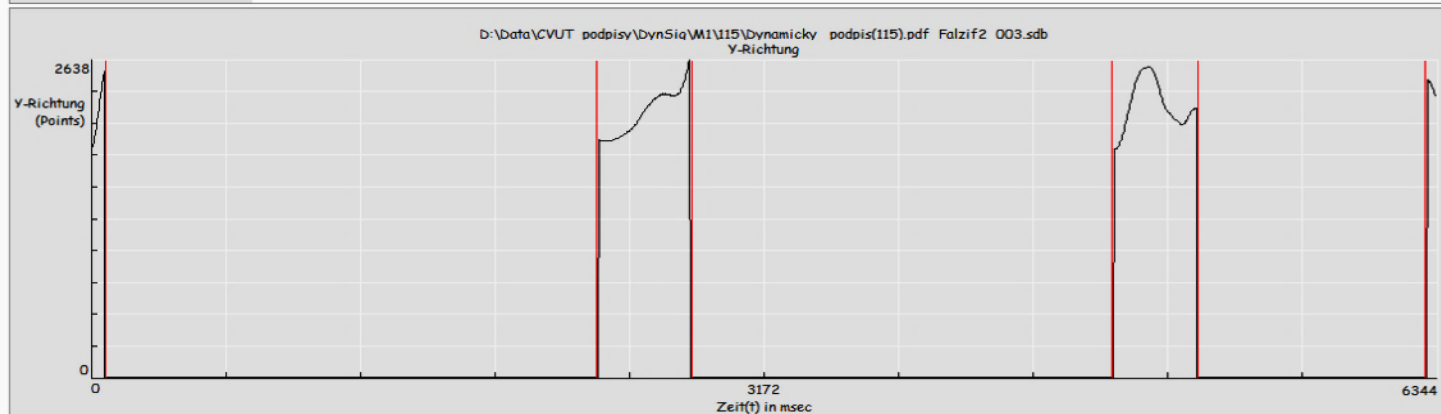


Dynamické charakteristiky

- Pao
- dyn
- V ra
- cha
- jejíž
- „pa
- Stej



Pokus o nápodobu podpisu dle vzoru
vykazuje diametrální odlišnosti v čase,
kdy byly vytvořeny vzor i padělek.



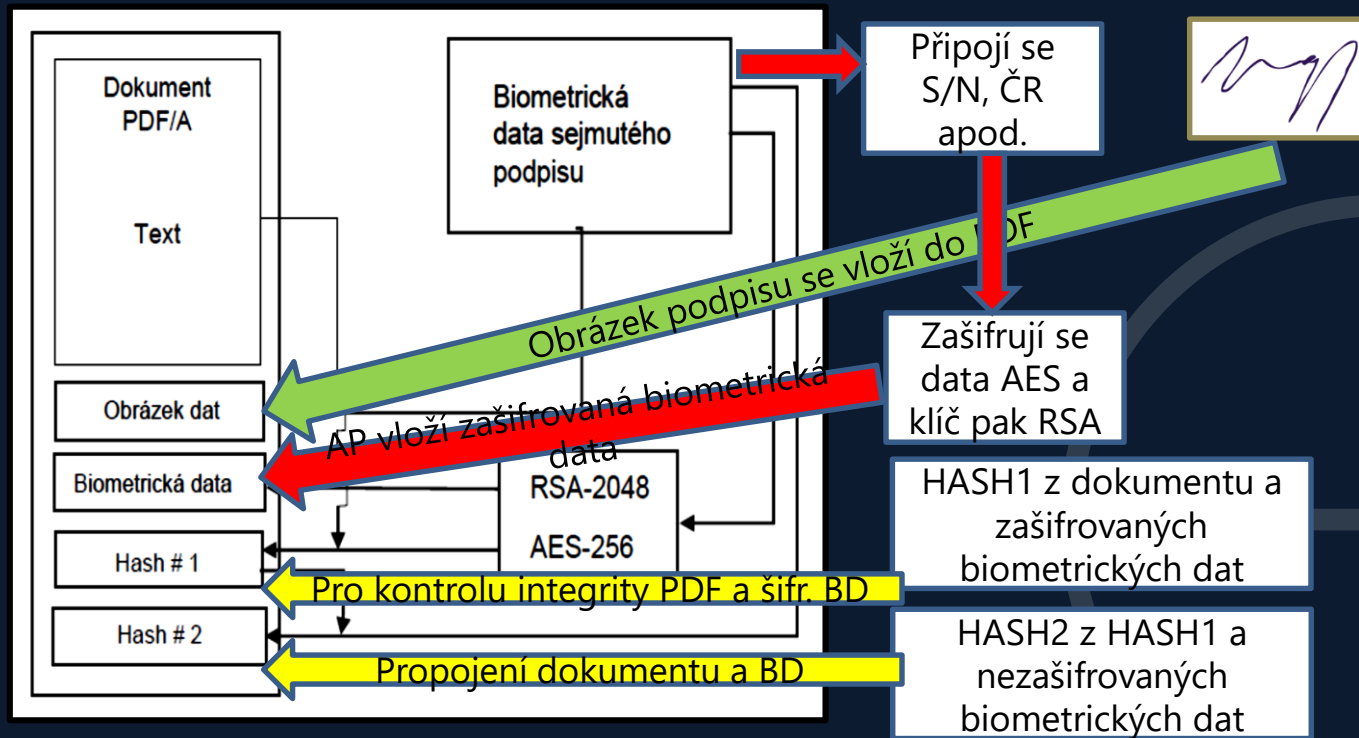
Využití dynamického podpisu

V případech kdy budou DBP sloužit jako **projev právního jednání** nebo v jiných situacích, kdy je přítomnost podpisu důležitá (**obchodní, pracovněprávní nebo zdravotnická dokumentace**), pak je nasazení této formy autentizace dokumentu vysoce přínosné jak pro rutinní využívání, tak pro zajištění integrity zpracovávaných podepsaných elektronických dokumentů. (EZ, ČR)



Zabezpečení DBP:

Schéma provázání DBP s dokumentem typu PDF



Dynamický biometrický podpis právně



DBP z hledis

**Uznávaný elektronický
podpis**

řízení eIDAS

- V čl. 3 najde
„Elektronický

podpis takto:
elektronické

**Zaručený elektronický
podpis**

**Kvalifikovaný
elektronický
podpis (ZEP s KvCt)**

Elektronický podpis

DBP z hlediska českého práva - NOZ

- § 561 - Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat. ... dříve z. č. 227/2000 Sb., nyní eIDAS a z. č. 297/2016 Sb. (komplikuje používání DBP **pro veřejnou sféru** vyžadováním KvEP a UzEP)
- § 562 Písemná forma je zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby.

DBP z hlediska českého práva - GDPR

- Slovo *biometrie* je původem z řečtiny a skládá se ze slov „*bios*“ a „*metron*“, přičemž slovo „*bios*“ znamená život a slovo „*metron*“ znamená měřítko. Jedná se tedy o jakési „měření života“.
- V oboru IT označujeme tímto výrazem systém či postup k rozpoznávání vzorů lidských vlastností.
- *Biometrie* (IT) je automatizované rozpoznávání lidských jedinců na základě jejich charakteristických *anatomických rysů* (např. obličej, otisk prstu, duhovka, sítnice) a *behaviorálních rysů* (tedy chování; např. dynamické vlastnosti podpisu, chůze). [DRAHANSKÝ, M. et al. *Biometrie*. Brno: Computer Press, s.r. o, 2011, s. 13]

DBP z hlediska českého práva - GDPR

Základní pojmy biometrie:

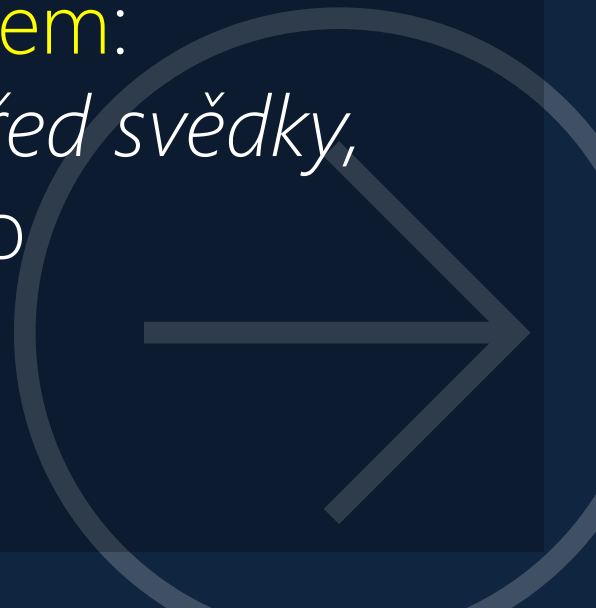
- Biometrické modality aneb čím je člověk charakterizován (typ biometrie).
- **Biometrická data - surová data nasnímaná čtečkou.**
- Biometrická šablona (resp. model) - digitalizovaná charakteristika rozpoznávané osoby - „vzhled“ (resp. „chování“).
- Biometrická reference - komplet šablon/modelů charakterizujících rozpoznávanou osobu.

DBP z hlediska českého práva - GDPR

- Rozpoznávání má ale dvě varianty užití:
- **Identifikací** rozumíme rozpoznání entity systémem, a to na základě určitého identifikátoru, který je spojen s určitou osobou, reprezentuje jeho identitu a může být znám jiným osobám. (Jméno a příjmení, případně další identifikátory, odstraňující zaměnitelnost... rodné číslo, číslo sociálního pojištění, bezvýznamový identifikátor atd.) Právně je identifikace **určení osoby, která učinila určitý úkon.**

DBP z hlediska českého práva - GDPR

- **Autentizace** znamená ověřování proklamované identity subjektu.
- Na listině – **vlastnoručním podpisem**:
podpisovým vzorem, podpisem před svědky, úředně ověřeným podpisem, nebo elektronickým podpisem.

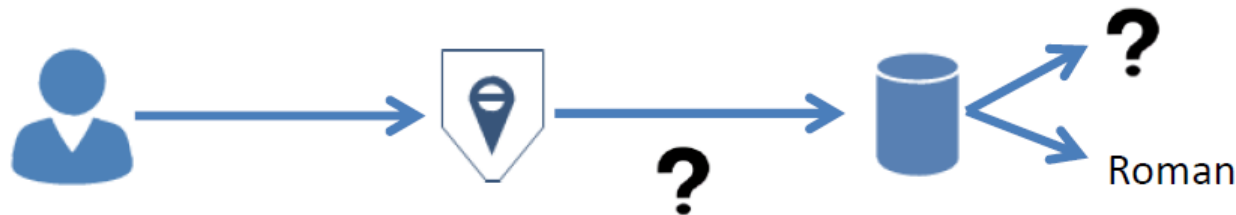


DBP z hlediska českého práva - GDPR

■ Autentizace (ověření identity)



■ Identifikace (forenzní aplikace)



DBP z hlediska českého práva - GDPR

Dynamický biometrický podpis

- Biometrie jako podpis



Data dynamického
biometrického
podpisu



„Biometrický“ podpis

- Biometrie jako
autentizace



Digitální podpis



DBP z hlediska českého práva - GDPR

Z. č. 101/2000 Sb.

citlivé údaje - osobní údaje vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů;

citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů (§ 4 písm. b).

GDPR

"biometrickými údaji" se rozumí osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo **znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje** (čl. 4 odst. 14)

DBP z hlediska českého práva - GDPR

- Podle § 9 citlivé údaje je možné zpracovávat, jen jestliže a) subjekt údajů dal ke zpracování výslovný **souhlas**, nebo h) je zpracování nezbytné pro **zajištění a uplatnění právních nároků**.
- ÚOOÚ (8. 8. 2016): **pokud tzv. dynamický biometrický podpis bude využíván stejně jako podpis klasický, tzn. jeho využití nebude spojeno s dalším automatickým zpracováním biometrických údajů** (např. porovnávání podpisu s podpisovým vzorem za využití biometrických dat), **bude se jednat o zpracování probíhající ve stejném právním režimu, jako při zpracování klasického podpisu. ...zpracování osobních, ale nikoliv citlivých údajů.**

Zakazuje se zpracování osobních údajů, které vypovídají o ... a zpracování genetických údajů, **biometrických údajů za účelem jedinečné identifikace fyzické osoby** a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.“ (čl. 9 odst. 1)

„Odst. 1 se nepoužije, pokud jde o některý z těchto případů: a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, ... f) **zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků** nebo pokud soudy jednají v rámci svých soudních pravomocí.“ (čl. 9 odst. 2)

DBP z hlediska českého práva - GDPR

- ÚOOÚ (8. 8. 2016): pokud tzv. dynamický biometrický podpis bude využíván stejně jako podpis klasický, tzn. jeho využití nebude spojeno s dalším automatickým zpracováním biometrických údajů (např. porovnávání s uloženým podpisovým vzorem), lze jeho zpracování o zpracování klasického podpisu stejnému právnímu režimu při zpracování klasického podpisu.

- ...zpracování osobních, ale nikoliv citlivých údajů

ÚOOÚ (8. 8. 2016): GDPR přináší podstatné právní změny. Zpracování osobních údajů, mj. biometrických, vyžaduje vytvoření vzoru (template) a jeho následné zpracování za účelem ověření totožnosti osob považuje za zpracování zvláštní kategorie osobních údajů...nebude tedy možno postupovat v mezích dosavadního stanoviska ÚOOÚ ... ÚOOÚ zveřejní aktuální stanovisko k biometrickým údajům.

Děje se něco nebo neděje?!

DBP z hlediska českého práva - GDPR

Podle našeho názoru:

DBP snímá „surová“ biometrická data, která jsou využívána pouze pro podepsání dokumentu, jejich využití nebude spojeno s dalším automatickým zpracováním biometrických údajů **a DBP není používán pro identifikaci subjektu údajů**. (Zásadní rozdíl: podpis autentizuje, identifikace probíhá jinak.)

Biometrické údaje jsou šifrovány, chráněny proti neoprávněnému přístupu a jsou zpřístupněny třetí osobě (soudnímu znalci) pouze v případě sporu o pravost podpisu, a to velmi formalizovaným postupem obsahujícím vysoké záruky.

Stále jde tedy o postup, který odpovídá dřívějšímu stanovisku ÚOOÚ - **ve stejném právním režimu, jako při zpracování klasického podpisu**. ...*nejde o zpracování biometrických údajů za účelem jedinečné identifikace fyzické osoby.*

Stanovisko ÚOOÚ č. 1/2017 – Biometrická identifikace nebo autentizace zaměstnanců

- **Přístupové systémy** – u přístupových systémů, kde zajištění bezpečnosti zpracováním citlivých biometrických údajů není stanoveno zvláštním zákonem prováděcí vyhláškou, lze **biometrické identifikace s vyhledáváním biometrických údajů v databázi použít jen s výslovným souhlasem jejich nositele** podle § 9 písm. a) z. č. 101/2000 Sb. (!)

Stanovisko ÚOOÚ č. 1/2017 – Biometrická identifikace nebo autentizace zaměstnanců

- **Docházkové systémy** – Jestliže dojde např. při použití jednosměrného hashování k vytvoření číselného údaje, jehož zpětná rekonstrukce na biometrický údaj není možná, nelze již tento údaj považovat za biometrický a využití takového systému může být v určitých případech přípustné i **bez souhlasu subjektu údajů, protože nedochází k uchovávání citlivého údaje**. Pro další zpracování údajů o docházce do zaměstnání za účelem plnění práv a povinností vyplývajících z pracovněprávních vztahů je v tom případě **aplikovatelná i výjimka z oznamovací povinnosti podle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů**.

Stanovisko ÚOOÚ č. 1/2017 – Biometrická identifikace nebo autentizace zaměstnanců

- Důležitým hlediskem je, zda je použitý otisk prstu (nebo jiná biometrická data) fyzické osoby, nebo na identifikaci subjektu údajů. Autentizační proces spočívá v porovnání údajů 1:1. Při autentizaci se srovnávají údaje i dalších osob, tedy výběrem z databáze, zatímco při identifikaci se srovnávají údaje pouze s jedinou osobou, tedy výběrem z databáze.
- Povinností zaměstnavatele je zajistit, aby biometrická data byla zpracovávána v souladu s GDPR. Proto nejlépe bude, pokud bude biometrická data uchovávána v oddělené databázi, která bude přístupná pouze pro účely autentizace, tedy metody ověření totožnosti. V tomto případě bude biometrická data uchovávána v oddělené databázi, která bude přístupná pouze pro účely autentizace, tedy metody ověření totožnosti. V tomto případě bude biometrická data uchovávána v oddělené databázi, která bude přístupná pouze pro účely autentizace, tedy metody ověření totožnosti.
- Rozhodné pro ÚOOÚ je, zda účelem použití otisku prstu, je pouze ověření totožnosti zaměstnance, nebo zda účelem použití otisku prstu, je pouze ověření totožnosti zaměstnance, nebo zda účelem použití otisku prstu, je pouze ověření totožnosti zaměstnance.

Kroutím nad tím hlavou... proč v červnu 2017 ÚOOÚ nepracuje alespoň duálně také s GDPR? (Návrh zákona o zpracování osobních údajů vše ponechává na GDPR.)

DBP z hlediska českého práva - GDPR

Závěry:

1. *eIDAS neohrozil DBP, spíše naopak,*
2. *právní úprava z. č. 297/2016 Sb, komplikuje používání DBP pro veřejnou sféru – PROČ?*
3. *GDPR by nemělo rovněž ohrozit používání DBP,*
4. *a už vůbec ne, pokud se bude jednat o zpracování se souhlasem nebo nezbytné pro určení, výkon nebo obhajobu právních nároků (čl. 9, odst. 2, písm. f) GDPR)*

dotazy ?

smejkal@znanoci.cz

