Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálny podpis

Ochrana dát a súkromia (Blok VII)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti vo verejnej správe

Ing. Ladislav Mariš, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

ladislav.maris@uniza.sk

Digitálny podpis (elektronický podpis)

- Klasický podpis
- Digitálny podpis
- Biometrický podpis = digitálny podpis s behaviorálnymi segmentami (rýchlosť, sklon, tlak ...)

- Zákonnosť
- Bezpečnosť

- Prečo? Papier, zelená doba, digitalizácia, veľké podniky, úrady, kuriér, ...)

Význam v bezpečnostnom kontexte

Webové technológie a bezpečnosť:

- Web je bežný komunikačný kanál aj v bezpečnostných systémoch
- Zraniteľnosti webových aplikácií môžu viesť k úniku citlivých údajov, manipulácii alebo narušeniu dôvery
- Bezpečné webové technológie sú základom pre digitálnu identitu, autentifikáciu (overenie) a elektronický podpis

Kľúčové pojmy:

- **Autenticita** – overenie totožnosti komunikujúcej strany
- **Integrita** – zaručenie nemennosti údajov
- **Dôveryhodnosť** – právne uznanie elektronickej komunikácie

Čo je digitálny podpis?

Definícia:

- Digitálny podpis (elektronický podpis) je kryptografická metóda na overenie pravosti a integrity elektronických údajov. **Nahrádza vlastnoručný podpis** v elektronickom prostredí.

Kľúčové pojmy (inak):

- **Autenticita** – zaručuje, že podpis vytvorila konkrétna osoba
- **Integrita** – obsah dokumentu nebol po podpise zmenený
- **Dôveryhodnosť** – autor nemôže poprieť, že podpísal dokument

Klasický podpis	Digitálny podpis
Rukou písaný	Elektronicky generovaný
Ľahko falšovateľný	Kryptograficky zabezpečený
Neumožňuje kontrolu obsahu	Zaručuje integritu dokumentu

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Právny rámec a typy elektronických podpisov

Zákonná úprava:

- **Nariadenie eIDAS (EU č. 910/2014)** – rámec pre elektronickú identifikáciu a dôveryhodné služby v EÚ
- **Zákon č. 272/2016 Z.z.** o dôveryhodných službách pre elektronické transakcie v SR
- **Zákon 215/2002 Z .z. o elektronickom podpise !!!**
- **A dalšie súvisiace predpisy**

Typy elektronických podpisov:

- Jednoduchý elektronický podpis - napr. napísané meno pod e-mailom
- Zaručený elektronický podpis - obsahuje kryptografickú ochranu a identifikáciu osoby
- **Kvalifikovaný elektronický podpis (KEP)** - právne rovnocenný s vlastnoručným podpisom, vytvorený cez kvalifikované zariadenie (napr. eID karta) - definovaný zákonom pri styku s verejnou mocou (úradmi)

Platnosť v praxi:

- KEP sa akceptuje pri podaniach na súdoch, úradoch a vo verejnej správe v celej EÚ (aj školy)

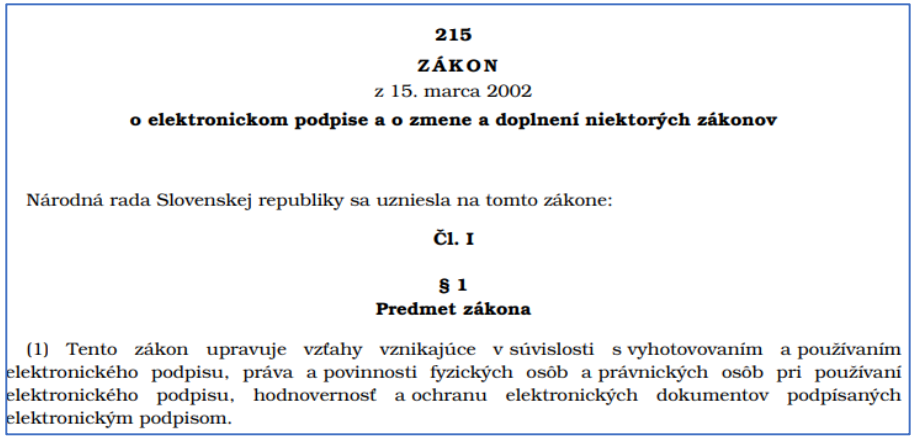
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kvalifikovaný elektronický podpis - KEP

- **Rovnocennosť s vlastnoručným podpisom:** Podľa nariadenia eIDAS platného v celej Európskej únii má kvalifikovaný elektronický podpis rovnaký právny účinok ako vlastnoručný podpis. To znamená, že dokumenty ním podpísané sú platné na úradoch, v bankách a pri iných právnych úkonoch.
- Zákon 215/2002 Z.Z. o elektronickom podpise:
- https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2002/215/vyhlasene_znenie.html

- Softvér pre používateľov elektronickej ID karty
- https://eidas.minv.sk/download/

- Doplňujúce predpisy: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2016/272/



215

ZÁKON

z 15. marca 2002

o elektronickom podpise a o zmene a doplnení niektorých zákonov

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

§ 1

Predmet zákona

(1) Tento zákon upravuje vzťahy vznikajúce v súvislosti s vyhotovovaním a používaním elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

215/2002 Z. z.

- upravuje vzťahy vznikajúce v súvislosti s **vyhotovovaním a používaním** elektronického podpisu, práva a povinnosti fyzických osôb a právnických osôb pri používaní elektronického podpisu, hodnovernosť a ochranu elektronických dokumentov podpísaných elektronickým podpisom
- Nesúvisí s utajovanými skutočnosťami (NBU SR)

§ 3 Elektronický podpis je **informácia pripojená alebo inak logicky spojená s elektronickým dokumentom**, ktorá musí spĺňať tieto požiadavky:

nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča a elektronického dokumentu; na základe znalosti tejto informácie a verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, **je zhodný s elektronickým dokumentom použitým na jej vyhotovenie.**

Zaručený elektronický podpis § 4 - 215/2002 Z. z.

- Elektronický podpis, ktorý je vyhotovený pomocou súkromného kľúča (určeného na vyhotovenie **ZEP**); možno ho vyhotoviť len s použitím bezpečného zariadenia; spôsob vyhotovenia umožňuje spoľahlivo určiť kto vyhotovil podpis; na verejný kľúč ktorý sa použil na vyhotovenie ZEP je vydaný kvalifikovaný platný certifikát (v čase vyhotovenia podpisu).

- Zaručený elektronický podpis úradu je platný, ak elektronický dokument, ku ktorému je zaručený elektronický podpis pripojený alebo s ním inak logicky spojený, je zhodný s dokumentom použitým na jeho vyhotovenie

- **Využívame pri styku s verejnou mocou** (úradmi)
- Overovateľ (úrad) overuje elektronický podpis aj pomocou verejného kľúča a na základe kvalifikovaného certifikátu

Certifikát verejného kľúča

- Elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený kľúč patrí osobe, ktorej je certifikát vydaný (skladá sa z tela a elektronického podpisu)

Obsahuje (telo certifikátu):

- identifikačné **údaje vydavateľa certifikátu**,
- identifikačné **číslo certifikátu**,
- identifikačné **údaje držiteľa certifikátu**,
- **dátum a čas začiatku a konca platnosti**,
- **verejný kľúč držiteľa** certifikátu,
- identifikáciu **algoritmov**, pre ktoré je uvedený verejný kľúč určený,
- identifikáciu algoritmov použitých pri vyhotovení elektronického podpisu tela certifikátu.

- Ako identifikačný údaj držiteľa certifikátu možno použiť aj **pseudonym**, ale len ak na základe údajov, ktoré certifikačná autorita pri podávaní žiadosti o vydanie certifikátu od žiadateľa získala, možno jednoznačne určiť totožnosť držiteľa certifikátu.

- Certifikačná autorita v certifikáte výslovne uvedie, že sa v ňom ako identifikačný údaj držiteľa certifikátu uvádza pseudonym.

Časová pečiatka podľa 215/2002 Z. z. § 9

Časová pečiatka je informácia pripojená alebo inak logicky spojená s elektronickým dokumentom, ktorá musí spĺňať tieto požiadavky:

- **nemožno ju efektívne vyhotoviť bez znalosti súkromného kľúča určeného na tento účel a bez elektronického dokumentu**,
- na základe znalosti verejného kľúča patriaceho k súkromnému kľúču použitému pri jej vyhotovení **možno overiť, že elektronický dokument, ku ktorému je pripojená alebo s ním inak logicky spojená, je zhodný s elektronickým dokumentom použitým na jej vyhotovenie**,
- vyhotovila ju akreditovaná certifikačná autorita použitím súkromného kľúča určeného na tento účel,
- možno ju vyhotoviť len použitím bezpečného zariadenia,
- na verejný kľúč patriaci k súkromnému kľúču použitému **na jej vyhotovenie vydala akreditovaná certifikačná autorita kvalifikovaný certifikát**,
- **umožňuje jednoznačne identifikovať dátum a čas, kedy bola vyhotovená.**

Slovenská národná certifikačná autorita SNCA

- Národná agentúra pre sieťové a elektronické služby (NASES) prostredníctvom **Slovenske j národnej certifikačnej autority (SNCA)** poskytuje bezodplatne kvalifikované dôveryhodné služby orgánom verejnej moci Slovenskej republiky

- https://www.nases.gov.sk/
- https://snca.gov.sk/

Technologické pozadie digitálneho podpisu

Kryptografické princípy:

- **Asymetrická kryptografia - Používa dvojicu kľúčov – súkromný kľúč** (na podpis) a **verejný kľúč** (na overenie podpisu)
- **Hašovacie funkcie - Prevod dokumentu na jedinečný reťazec (napr. SHA-256). Zaručuje integritu údajov.**

Algoritmy:

- **RSA** (Rivest Shamir Adleman)
- **DSA** (Digital Signature Algorithm)
- **ECC** (Elliptic Curve Cryptography)

Certifikáty a certifkačná autorita:

- **Digitálny certifikát** – overuje, komu patrí verejný kľúč
- **Certifikačná autorita (CA)** – dôveryhodná tretia strana, ktorá certifikát vydáva

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako funguje digitálny podpis – proces

1. Vytvorenie podpisu:

- Z dokumentu sa vygeneruje hash (napr. SHA-256)
- Hash sa zašifruje **súkromným kľúčom** – vzniká digitálny podpis
- Dokument a podpis sa odošlú príjemcovi

2. Overenie podpisu:

- Príjemca z dokumentu opäť vygeneruje hash
- Rozšifruje prijatý podpis **verejným kľúčom** – získa pôvodný hash
- Porovnávanie hashov navzájom

➤ **Zhodujú sa? →**

dokument je autentický a nebol zmenený

Využitie digitálneho podpisu v praxi

1. **Štátna správa a verejný sektor**
   - **Slovensko.sk**, elektronické podania na súdy a úrady
   - Daňové priznania, prihlášky, žiadosti, odvolania
   - Použitie **eID karty** s KEP (kvalifikovaný elektronický podpis)
2. **Firemné a osobné využitie**
   - Elektronické zmluvy a faktúry
   - Digitálne podpisovanie PDF dokumentov (napr. Adobe Acrobat, D.Signer)
   - Autentifikácia pri prístupe do firemných systémov
3. **E-mailová bezpečnosť**
   - Podpisovanie a šifrovanie e-mailov
   - Zabezpečená výmena citlivých informácií
4. **Webové aplikácie**
   - Podpisovanie XML a JSON dokumentov (napr. vo verejných API)
   - Integrácia eIDAS podpisových služieb do webových rozhraní

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Digitálny podpis vo webových aplikáciách

Prečo podpisovanie vo webovom prostredí?

- Overenie identity používateľa
- Právne záväzné úkony cez internet (napr. podpisovanie zmlúv)
- Dôvera v elektronické služby a formuláre

Možnosti implementácie:

- **Integrácia cez API** (napr. eIDAS, DocuSign, Adobe Sign)
- **Klientské podpisovanie** (napr. eID karta + aplikácia)
- **Serverové podpisovanie** pomocou kvalifikovaného certifikátu

Technické výzvy:

- Prístup k súkromnému kľúču na klientskom zariadení
- Riešenie bezpečnosti v prehliadači (napr. obmedzenia JavaScriptu)
- Kompatibilita s rôznymi zariadeniami a OS

Príklad použitia:

- Vyplnenie formulára online → podpis KEP → odoslanie na server → uloženie do systému

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Bezpečnostné riziká a odporúčania

Hrozby pri používaní digitálneho podpisu:

- **Phishing** – získanie prihlasovacích údajov alebo falošný podpisový portál
- **Man-in-the-Middle (MITM)** – odchytenie a pozmenenie komunikácie medzi používateľom a serverom
- **Keylogger** – sledovanie klávesnice a krádež PIN-u alebo hesla
- **Zneužitie súkromného kľúča** – pri slabom zabezpečení zariadenia alebo úložiska

Odporúčania pre bezpečné používanie:

- Používať **HTTPS** a dôveryhodné certifikáty na všetkých weboch
- Nikdy nezdieľať súkromný kľúč alebo PIN
- Overovať dôveryhodnosť podpisového prostredia (certifikáty, CA)
- Využívať **kvalifikované podpisové zariadenia** (napr. čítačka + eID karta)
- Pravidelne **aktualizovať softvér** a antivírusové riešenia

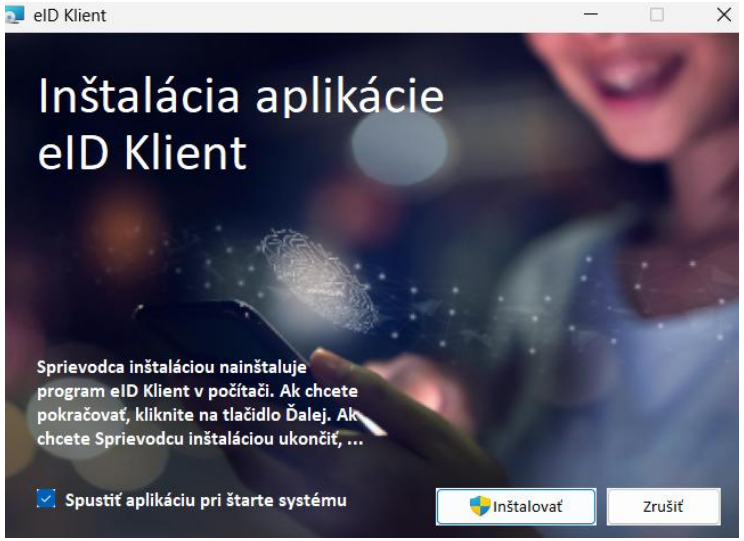
Dôležité:

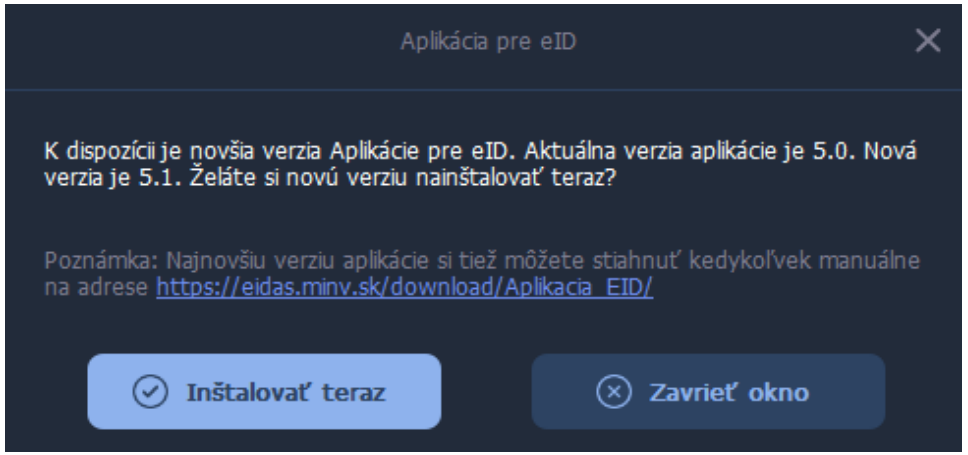
- Bezpečnosť digitálneho podpisu nie je len o technológii, ale aj o správaní používateľa.

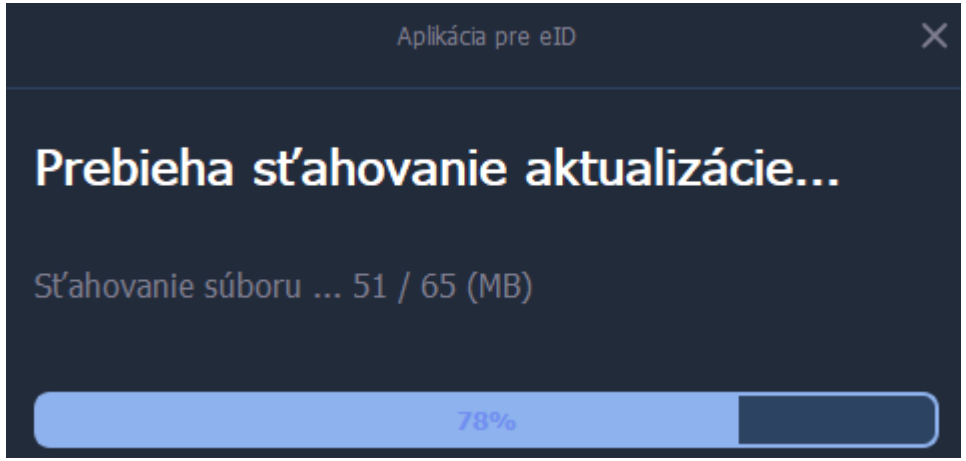
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ukážka zriadenia elektronického podpisu

- EID klient





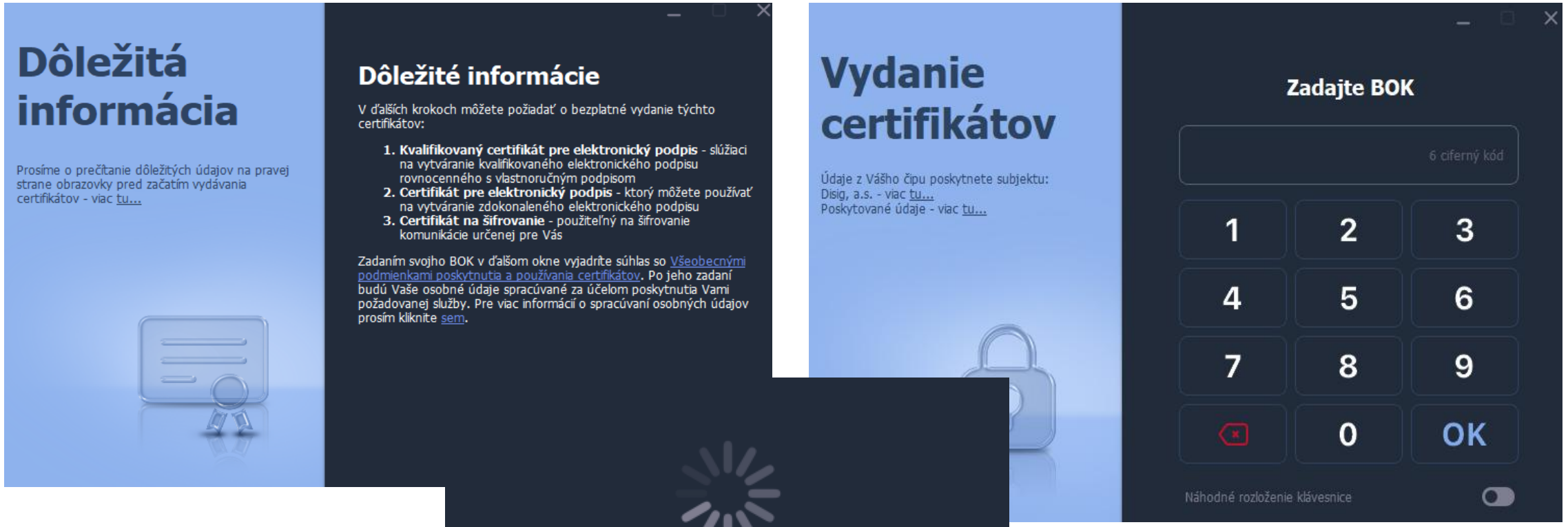


https://www.youtube.com/watch?v=ek-3_stz9iU

https://www.slovensko.sk/sk/na-stiahnutie

https://www.slovensko.sk/sk/na-stiahnutie/aplikacie-pre-kvalifikovany-el

Ukážka

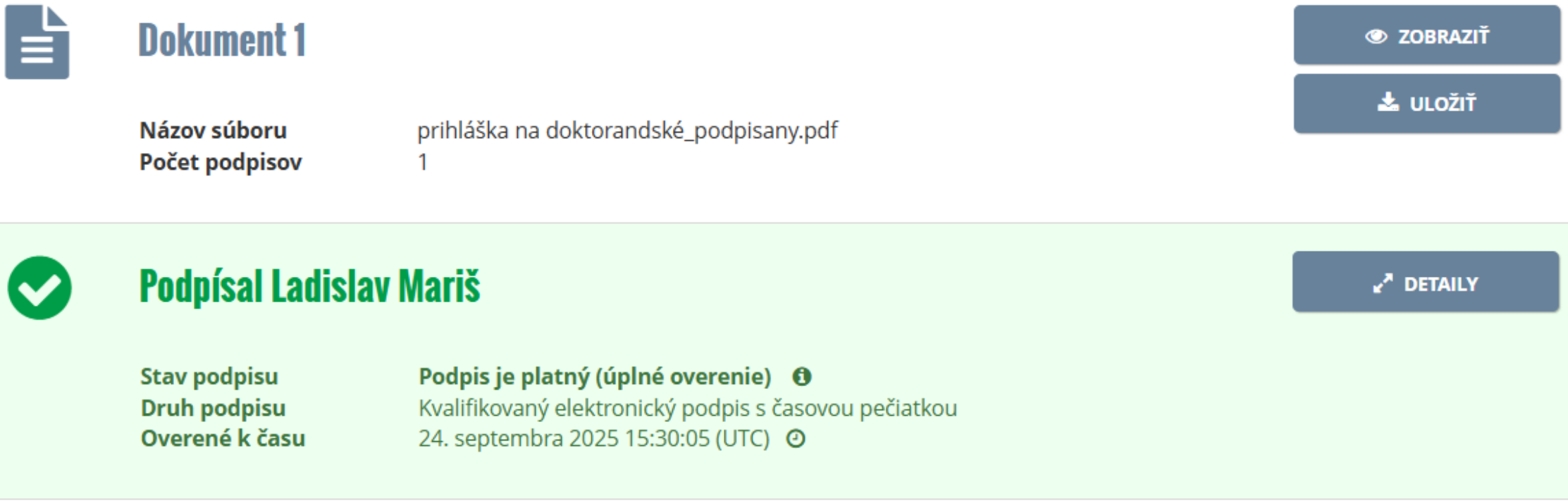


https://www.qesportal.sk/

https://www.slovensko.sk/sk/e-sluzby/sluzba-overenia-zep

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

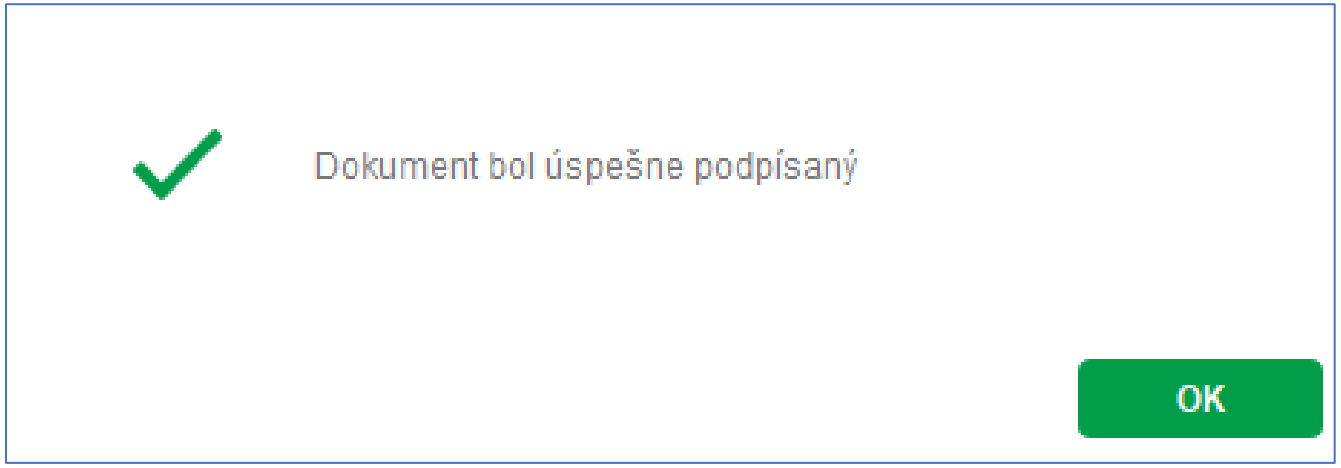
Overenie



- https://www.youtube.com/watch?v=c65D3LEFkl8

Zhrnutie

- Digitálny podpis je **kľúčovým prvkom bezpečnosti** v digitálnom svete
- Právny rámec (eIDAS, ZEP/KEP) zabezpečuje **dôveru a uznanie podpisu v celej EÚ**
- **Bezpečná implementácia a správne návyky** sú nevyhnutné pre ochranu



https://youtu.be/UhjEcFT_mI0

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ZHRNUTIE https://youtu.be/UhjEcFT_mI0

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Otázky?

- Aké riziká vnímate pri digitálnom podpise?
- Poznáte systémy, ktoré už používajú elektronický podpis?
- Čo je to digitálny občiansky preukaz a aký je súvis s digitálnou identitou?

§ 3a Digitálny občiansky preukaz

(1) Občan Slovenskej republiky si môže vytvoriť digitálny rovnopis svojho občianskeho preukazu (ďalej len „digitálny občiansky preukaz“) prostredníctvom mobilnej aplikácie v správe Ministerstva vnútra Slovenskej republiky (ďalej len „ministerstvo“).

(2) Údaje uvedené v digitálnom občianskom preukaze možno overiť len prostredníctvom overovacej mobilnej aplikácie v správe ministerstva.

(3) Predloženie digitálneho občianskeho preukazu osobe, ktorá má k dispozícii overovaciu mobilnú aplikáciu podľa odseku 2 a sú u nej splnené technické podmienky jej používania, má rovnaké účinky ako predloženie občianskeho preukazu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Doplnkové zdroje

Videá:
https://www.youtube.com/watch?v=cd8vRFR0q_g
https://www.youtube.com/watch?v=TACQ_ehIaT8
https://www.youtube.com/watch?v=zBhj2ZO7HqY

Slovensko.sk
https://www.slovensko.sk/sk/na-stiahnutie/aplikacie-pre-kvalifikovany-el
https://www.slovensko.sk/sk/slovnik/detail/_elektronicky-podpis

Zákon č. 272/2016 Z.z. v znení neskorších predpisov (2017) + elektronický podpis
https://www.slov-lex.sk/ezbierky/vyhladavanie-pravnych-predpisov?hladanyVyraz=elektronick%C3%BD+podpis

Digitálny podpis
https://www.slov-lex.sk/ezbierky/vyhladavanie-pravnych-predpisov?hladanyVyraz=digit%C3%A1lny+podpis

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Ochrana dát a súkromia

Digitálny podpis (Blok VII)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ing. Ladislav Mariš, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

ladislav.maris@uniza.sk