
KVALIFIKOVANÝ ELEKTRONICKÝ PODPIS, ČASOVÁ PEČIATKA A MANDÁTNY CERTIFIKÁT ZÁKLADY



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. Právny a Koncepčný Rámec

- Nariadenie eIDAS: Jednotný digitálny trh
- Vnútroštátna legislatíva: Zákon o dôveryhodných službách a Zákon o e-Governmente
- Od Zaručeného (ZEP) k Kvalifikovanému (KEP) Podpisu

2. Kvalifikovaný Elektronický Podpis (KEP)

- Definícia a právna sila
- Základné vlastnosti: Autenticita, Integrita, Nepopierateľnosť
- Technické predpoklady: QSCD

3. Kvalifikovaná Elektronická Časová Pečiatka

- Účel a definícia podľa eIDAS
- Význam pre dlhodobú platnosť (LTV)

OBSAH

4. Mandátny Certifikát a Elektronická Pečať

- Mandátny certifikát: Konanie v mene iného
- Kvalifikovaná elektronická pečať (KEPe)
- Praktické rozlíšenie použitia

5. Praktické Postupy: Od Teórie k Aplikácii

- Sprevádzkovanie KEP na eID
- Podpisovanie dokumentov
- Získanie mandátneho certifikátu a použitie časovej pečiatky

6. Zdroje, Návod a Riešenie Problémov

7. Súvisiace Koncepty a Budúci Vývoj

- Zaručená konverzia, GDPR a eIDAS 2.0

PRÁVNÝ A KONCEPČNÝ RÁMEC

Nariadenie eIDAS: Základný Kameň Dôvery v EÚ

- **Celý názov:** Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014, známe ako **eIDAS**.
- **Hlavný cieľ:** Odstrániť bariéry v cezhraničných elektronických transakciách a vybudovať jednotný digitálny trh.
- **Kľúčová vlastnosť:** Na rozdiel od smerníc je **priamo aplikovateľné** vo všetkých členských štátoch EÚ.
- Harmonizuje pravidlá pre dôveryhodné služby ako sú elektronické podpisy, pečate a časové pečiatky.

ÚROVNE ELEKTRONICKÝCH PODPISOV PODĽA EIDAS

Nariadenie eIDAS definuje tri základné úrovne elektronických podpisov:

- **Elektronický podpis (jednoduchý)**
 - Dáta v elektronickej forme pripojené k iným dátam, ktoré podpisovateľ používa na podpisovanie.
 - Príklad: Meno napísané na konci e-mailu, naskenovaný podpis.
 - Najnižšia právna istota.
- **Zdokonalený elektronický podpis (AdES)**
 - Musí byť jedinečne spojený s podpisovateľom a umožniť jeho identifikáciu.
 - Zabezpečuje, že akákoľvek zmena v dátach je zistiteľná.
- **Kvalifikovaný elektronický podpis (KEP)**
 - Najvyššia úroveň. Je to zdokonalený podpis vytvorený pomocou kvalifikovaného zariadenia (QSCD) a založený na kvalifikovanom certifikáte.

PRINCÍP VZÁJOMNÉHO UZNÁVANIA

"Jeden podpis vládne všetkým (v EÚ)"

- Absolútne kľúčový princíp, ktorý eIDAS zavádza.
- Podľa článku 25 ods. 3: Kvalifikovaný elektronický podpis založený na kvalifikovanom certifikáte vydanom v jednom členskom štáte **sa uznáva ako kvalifikovaný elektronický podpis vo všetkých ostatných členských štátoch.**
- **V praxi to znamená:** Váš KEP vytvorený slovenským eID je rovnako platný pri komunikácii s nemeckým partnerom, španielskym úradom alebo pri akejkoľvek inej právne relevantnej transakcii v rámci EÚ.

VNÚTROŠTÁTNA LEGISLATÍVA V SR

Hoci je eIDAS priamo aplikovateľné, Slovensko má dva kľúčové doplňujúce zákony:

1. Zákon č. 272/2016 Z. z. o dôveryhodných službách

- Hlavný implementačný predpis k eIDAS.
- Definuje "ako" sa pravidlá uplatňujú v SR (napr. pôsobnosť NBÚ ako orgánu dohľadu).

2. Zákon č. 305/2013 Z. z. o e-Governmente

- Zameriava sa na procesnú stránku komunikácie so štátom.
- Definuje elektronické podania, elektronické schránky a zaručenú konverziu.

eIDAS hovorí "ČO", národné zákony hovoria "AKO".

OD ZEP K KEP: PRÁVNÁ KONTINUITA

- Pred rokom 2016 sa v SR používal termín **Zaručený elektronický podpis (ZEP)**.
- Zmena terminológie zo ZEP na KEP bola primárne zosúladením s legislatívou EÚ, nie zmenou právnej sily.
- **Zákonná kontinuita je zabezpečená:** § 17 Zákona č. 272/2016 Z. z. stanovuje, že kdekoľvek sa v zákonoch spomína ZEP, rozumie sa tým KEP.
- Všetky dokumenty podpísané ZEP-om pred 18. októbrom 2016 **zostávajú plne platné**.

POROVNANIE ZEP A KEP

ATRIBÚT	ZARUČENÝ ELEKTRONICKÝ PODPIS (ZEP)	KVALIFIKOVANÝ ELEKTRONICKÝ PODPIS (KEP)
Právny základ	Zákon č. 215/2002 Z. z. (zrušený)	Nariadenie (EÚ) č. 910/2014 (eIDAS) a Zákon č. 272/2016 Z. z.
Právny účinok	Ekvivalent vlastnoručného podpisu	Ekvivalent vlastnoručného podpisu
Medzinárodné uznanie	Obmedzené, závislé od dohôd	Povinné vzájomné uznávanie v celej EÚ
Súčasný stav	Starší, legislatívne nahradený termín	Aktuálna a správna terminológia

KVALIFIKOVANÝ ELEKTRONICKÝ PODPIS (KEP)

Definícia a Právna Sila

- KEP je najvyššia a právne najzáväznejšia forma elektronického podpisu v EÚ.
- Je definovaný ako **zdokonalený elektronický podpis**, ktorý je:
 1. Vyhotovený s použitím **kvalifikovaného zariadenia (QSCD)**.
 2. Založený na **kvalifikovanom certifikáte**.
- **Najdôležitejší právny dôsledok (Čl. 25 ods. 2 eIDAS):**

"Kvalifikovaný elektronický podpis má právny účinok **rovnocenný s vlastnoručným podpisom**."
- Podpisovateľom môže byť **výlučne fyzická osoba**, pretože len tá môže prejaviť svoju vôľu.

ZÁKLADNÉ VLASTNOSTI KEP

Právna sila KEP sa opiera o tri kryptograficky zabezpečené vlastnosti:

- **Autenticita (Kto podpísal?)**
 - Zaručuje, že je možné jednoznačne overiť identitu osoby, ktorá podpis vytvorila.
 - **Integrita (Čo bolo podpísané?)**
 - Zabezpečuje, že podpísaný dokument nebol po vytvorení podpisu žiadnym spôsobom zmenený. Aj zmena jedinej bodky by viedla k neplatnosti podpisu.
 - **Nepopierateľnosť (Naozaj to podpísal on?)**
 - Autor podpisu nemôže neskôr úspešne tvrdiť, že podpis nevytvoril, pretože jeho súkromný kľúč je pod jeho výlučnou kontrolou na QSCD.
-

TECHNICKÉ PREDPOKLADY PRE KEP

Vysoká dôvera v KEP je podmienená hardvérovou a procesnou bezpečnosťou.

- **Kvalifikovaný certifikát:** Vydáva ho kvalifikovaný poskytovateľ po dôkladnom overení identity žiadateľa. Spája identitu osoby s jej verejným kľúčom.
- **Kvalifikované zariadenie (QSCD):** Certifikovaný hardvér, ktorý bezpečne uchováva súkromný kľúč podpisovateľa.
 - V SR je najrozšírenejším QSCD **čip na elektronickom občianskom preukaze (eID karta)**.
- **Dvojfaktorová autentizácia:** Kombinácia:
 1. **Vlastníctva:** Fyzická eID karta.
 2. **Znalosti:** 6-miestny **KEP PIN**.

KVALIFIKOVANÁ ELEKTRONICKÁ ČASOVÁ PEČIATKA

Prečo potrebujeme časovú pečiátku?

- KEP odpovedá na otázky "kto?" a "čo?", ale **neposkytuje dôkaz o tom, "kedy"** bol dokument podpísaný.
- Čas v počítači používateľa nemá žiadnu dôkaznú hodnotu.
- **Definícia (eIDAS):** Údaje v elektronickej forme, ktoré viažu iné údaje s konkrétnym časom, čím tvoria dôkaz o existencii týchto údajov v danom čase.
- Funguje ako služba **dôveryhodnej tretej strany (TSA)**.

PRÁVNE ÚČINKY A VÝZNAM PRE LTV

- **Právna domnienka:** Pri kvalifikovanej časovej pečiatke platí **právna domnienka správnosti dátumu a času**, ktorý uvádza, a integrity údajov. Dôkazné bremeno je na strane, ktorá by to chcela spochybniť.
- **Dlhodobá Archivácia (Long-Term Validation - LTV):**
 - Časová pečiatka rieši problém expirácie podpisových certifikátov.
 - "Zmrazí" platnosť podpisu v čase jej vydania, čím potvrdzuje, že podpis bol v danom momente platný.
 - Bez časových pečiatok je dlhodobá právna hodnota elektronických dokumentov vážne ohrozená.

ÚROVNE DLHODOBEJ PLATNOSTI (LTV)

Pre zabezpečenie overiteľnosti na desiatky rokov sa používajú pokročilé formáty podpisov (ETSI baseline profily):

- **B-T (Timestamp):**
 - K základnému podpisu (B-B) sa pridá **časová pečiatka**.
- **B-LT (Long-Term):**
 - K B-T úrovni sa pridajú všetky potrebné **revokačné údaje** (zoznamy zneplatnených certifikátov) a celá **certifikačná cesta**. Umožňuje overenie aj offline.
- **B-LTA (Long-Term with Archive):**
 - K B-LT úrovni sa pridáva ďalšia, **archívna časová pečiatka**, ktorá chráni celý balík (pôvodný podpis, prvú pečiatku aj revokačné údaje). Tento proces sa môže periodicky opakovať.

MANDÁTNY CERTIFIKÁT

Konanie v mene iného subjektu

- V digitálnom svete nahrádza pripojenie funkcie k podpisu (napr. "Ján Vážny, konateľ").
 - **Definícia:** Kvalifikovaný certifikát vydaný fyzickej osobe, ktorý okrem jej identity obsahuje aj údaje o subjekte (mandantovi), v mene ktorého koná, a o rozsahu oprávnenia (mandáte).
 - Informácia o zastúpení je takto priamo a neoddeliteľne kryptograficky spojená s podpisom.
 - **Určený pre:**
 - Štatutárov, predstaviteľov verejnej moci, slobodné povolania (advokáti, notári), poverených zamestnancov.
-

KVALIFIKOVANÁ ELEKTRONICKÁ PEČAŤ (KEPE)

- Elektronický podpis môže vyhotoviť iba fyzická osoba. Pre právnické osoby slúži **KEPe**.
- Technický ekvivalent KEP, avšak certifikát je viazaný na **právnickú osobu**.
- **Hlavný účel:**
 - Zabezpečiť **pôvod a integritu** dokumentu.
 - Slúži ako digitálny ekvivalent **oficiálnej pečiatky organizácie**, nepotvrdzuje vôľu konkrétnej osoby.
- **Použitie:** Často v automatizovaných procesoch, ako je generovanie faktúr, vydávanie potvrdení o prijatí, pečatenie výpisov z registrov.

KEDY POUŽIŤ MANDÁTNY CERTIFIKÁT A KEDY PEČAŤ?

Nesprávne použitie autorizačného nástroja môže viesť k neplatnosti dokumentu. Rozhoduje vždy požiadavka konkrétneho zákona.

- **KEP s Mandátnym certifikátom sa MUSÍ použiť, ak:**
 - Osobitný zákon vyžaduje, aby bol dokument **podpísaný konkrétnou osobou alebo osobou v konkrétnej funkcii** (napr. "rozhodnutie podpisuje starosta"). Pečať nestačí, lebo nevyjadruje osobnú zodpovednosť.
- **Kvalifikovaná elektronická pečať (KEPe) sa MÔŽE použiť, ak:**
 - Osobitný zákon **nevyžaduje podpis konkrétnej osoby**, ale iba autorizáciu dokumentu ako celku danou inštitúciou.

SÚHRNNÉ ROZLIŠENIE POUŽITIA

Nástroj	Subjekt	Účel	Príklad Použitia
KEP (štandardný)	Fyzická osoba	Konanie vo vlastnom mene, vyjadrenie osobnej vôle.	Občan podáva daňové priznanie.
KEP s Mandátnym certifikátom	Fyzická osoba v mene iného subjektu	Preukázanie oprávnenia konať za inú osobu/inštitúciu.	Starosta podpisuje VZN. Konateľ podpisuje zmluvu v mene s.r.o..
KEPe (pečať)	Právnická osoba / OVM	Preukázanie pôvodu a integrity dokumentu od organizácie.	Mesto automaticky vydáva potvrdenie o prijatí podania. E-shop pečatí faktúru.

SPREVÁDZKOVANIE KEP NA EID (KROK 1)

Proces je bezplatný a dostupný pre občanov SR s eID.

Krok 1: Čo potrebujete?

- Počítač (Windows, macOS, Linux)
- Pripojenie na internet
- Čítačka čipových kariet (externá alebo integrovaná)
- eID karta (občiansky preukaz s čipom)
- Bezpečnostný osobný kód (BOK), ktorý ste si zvolili pri preberaní OP

SPREVÁDZKOVANIE KEP NA EID (KROK 2)

Krok 2: Inštalácia softvéru

1. Navštívte **www.slovensko.sk** a prejdite do sekcie "**Na stiahnutie**".
2. Stiahnite a nainštalujte:
 - Ovládače k čítačke (ak je to potrebné).
 - Aplikáciu pre eID (**eID klient**).
 - Aplikáciu pre KEP (**D.Suite/eIDAS** alebo **D.Launcher** pre macOS/Linux).
3. Po inštalácii **reštartujte počítač**.

SPREVÁDZKOVANIE KEP NA EID (KROK 3)

Krok 3: Aktivácia a vydanie certifikátov

- Tento krok je možné vykonať aj dodatočne online, ak ste tak neurobili pri prevzatí OP.
 1. Pripojte čítačku a vložte eID kartu.
 2. Spustíte aplikáciu **eID klient**.
 3. Prihláste sa zadaním **BOK** kódu.
 4. Aplikácia zistí stav certifikátov. Ak chýbajú, ponúkne možnosť "**Vydať certifikáty**".
 5. V sprievodcovi si nastavíte dva nové kódy:
 - **KEP PIN (6 číslic)**: Na potvrdzovanie podpisu.
 - **KEP PUK (8 číslic)**: Na odblokovanie KEP PIN-u.
 6. Po úspešnom procese sa certifikáty zapíšu na čip vašej eID karty.

PREHLÁD BEZPEČNOSTNÝCH KÓDOV PRE EID

Názov kódu (Skratka)	Dĺžka	Počet Pokusov	Odblokovanie
Bezpečnostný osobný kód (BOK)	6 číslic	Autentifikácia: Prihlasovanie na portály (slovensko.sk).	5 PUK kódom alebo osobne na oddelení dokladov.
KEP PIN	6 číslic	Autorizácia: Potvrdenie vytvorenia každého KEP.	3 Pomocou KEP PUK kódu v aplikácii eID klient.
KEP PUK	8 číslic	Odblokovanie: Slúži výhradne na odblokovanie zablokovaného KEP PIN-u.	3 Iba osobne na oddelení dokladov.

Je dôležité rozumieť rozdielu medzi kódmi, aby ste si nezablokovali prístup.

PODPISOVANIE DOKUMENTOV (D.SUITE/EIDAS)

Príklad: Podpisovanie na portáli www.slovensko.sk

- 1. Prihlásenie:** Prihláste sa na portál pomocou eID a BOK kódu.
- 2. Služba:** Vyplňte formulár (napr. Všeobecná agenda) a priložte dokumenty (.pdf, .xml, .txt).
- 3. Iniciovanie podpisu:** Pri prílohe kliknite na tlačidlo "**Podpísať**".
- 4. Aplikácia D.Signer:** Spustí sa lokálna aplikácia. Zobrazí náhľad dokumentu a vyzve vás na zadanie **KEP PIN** kódu.
- 5. Odoslanie:** Po podpísaní všetkých príloh odošlite celé podanie.

Pozn.: Pre komunikáciu s OVM v SR sa z historických dôvodov najčastejšie používa formát **XAdES** (.zep, .xzep).

ZÍSKANIE MANDÁTNEHO CERTIFIKÁTU

Proces je administratívne náročnejší, pretože sa overuje aj oprávnenie konať.

- 1. Výber poskytovateľa:** Vyberte si jedného z komerčných kvalifikovaných poskytovateľov (napr. Disig, I.CA).
 - 2. Podanie žiadosti:** Vyplňte žiadosť.
 - 3. Doloženie mandátu:** Musíte preukázať svoje oprávnenie:
 - **Štatutári:** Výpis z Obchodného registra.
 - **Predstavitelia OVM:** Menovací dekrét.
 - **Slobodné povolania:** Potvrdenie od príslušnej komory (napr. SAK, SKA).
 - **Zamestnanci:** Úradne osvedčené splnomocnenie.
 - 4. Overenie identity:** Osobná návšteva u poskytovateľa.
 - 5. Vydanie certifikátu:** Certifikát sa nahrá na bezpečné zariadenie (QSCD) – napr. čipovú kartu alebo USB token.
-

VYUŽITIE KVALIFIKOVANEJ ČASOVEJ PEČIATKY

Na rozdiel od KEP na eID je táto služba **komerčná a spoplatnená**.

- 1. Nákup služby:** Zakúpite si balík časových pečiatok od kvalifikovaného poskytovateľa (napr. 500 ks).
- 2. Prístupové údaje:** Dostanete prístupové údaje k serveru časových pečiatok (TSA).
- 3. Konfigurácia:** Údaje nastavíte vo svojej podpisovacej aplikácii (napr. Disig Desktop Signer, QSign).
- 4. Použitie:** Pri podpisovaní aplikácia automaticky pripojí k podpisu aj časovú pečať.

Použitie je povinné pri podaniach na súdy alebo v katastrálnom konaní a dôrazne odporúčané pre všetky zmluvy a dôležité dokumenty s dlhodobou platnosťou.

ZDROJE A DÔLEŽITÉ ODKAZY

- **Ústredný portál verejnej správy (ÚPVS):**
 - <https://www.slovensko.sk>
 - Hlavný vstupný bod pre e-komunikáciu so štátom.
- **Softvér na stiahnutie (eID klient, D.Suite/eIDAS):**
 - <https://www.slovensko.sk/sk/na-stiahnutie>
- **Návody a podpora:**
 - Oficiálne návody ÚPVS: <https://www.slovensko.sk/sk/navody>
 - Komunitné návody: <https://navody.digital>
- **Informácie o eID karte:**
 - Ministerstvo vnútra SR: <https://www.minv.sk/?obcianske-preukazy>

ZOZNAM KVALIFIKOVANÝCH POSKYTOVATEĽOV

- Trh s mandátnymi certifikátmi, pečat'ami a časovými pečiatkami je komerčný.
- **Oficiálny zoznam poskytovateľov ("Trusted List"):**
 - Vedie ho a zverejňuje **Národný bezpečnostný úrad (NBÚ)** ako orgán dohľadu.
 - Adresa: <https://www.nbu.gov.sk/doveryhodne-zoznamy/>.
 - Tento zoznam zaručuje, že poskytovateľ má kvalifikovaný štatút a jeho služby sú interoperabilné v celej EÚ.
- **Príklady komerčných poskytovateľov na Slovensku:**
 - Disig, a.s.
 - První certifikační autorita, a.s. (I.CA)
 - NFQES (BRAIN:IT)
 - PSCA, s.r.o.

RIEŠENIE NAJČASTEJŠÍCH PROBLÉMOV (1/2)

Problém: Prihlásenie alebo podpisovanie nefunguje.

- **Možné príčiny a riešenia:**

- **Neaktuálny softvér:** Uistite sa, že máte najnovšiu verziu eID klienta a D.Suite/eIDAS zo slovensko.sk.
- **Problém s čítačkou:** Skúste iný USB port, preinštalujte ovládače.
- **Neaktívne rozšírenie v prehliadači:** Skontrolujte, či je v prehliadači povolené rozšírenie D.Bridge 2.
- **Konflikt s antivírusom:** Dočasne deaktivujte antivírus alebo pridajte výnimku.
- **"IT Crowd" riešenie:** Reštartujte aplikáciu eID klient a potom celý počítač.

RIEŠENIE NAJČASTEJŠÍCH PROBLÉMOV (2/2)

Problém: Systém hlási "Neplatný podpis".

- **Možné príčiny a riešenia:**

- **Problém na strane prijímateľa:** Problém nemusí byť na vašej strane. Informačný systém úradu nemusí byť správne nakonfigurovaný.
- **Exspirovaný certifikát:** Overte platnosť certifikátov cez eID klient.
- **Nesprávny formát podpisu:** Uistite sa, že používate formát, ktorý prijímajúci systém akceptuje (pre OVM v SR zvyčajne XAdES).

Problém: Zablokovaný KEP PIN.

- **Riešenie:** Po 3 neúspešných pokusoch sa PIN zablokuje. Na odblokovanie použite aplikáciu **eID klient** a 8-miestny **KEP PUK** kód. Následne si nastavíte nový KEP PIN. Ak zablokujete aj KEP PUK, je nutná **osobná návšteva oddelenia dokladov**.

ZARUČENÁ KONVERZIA

Právny "most" medzi listinným a elektronickým svetom

- **Definícia:** Proces transformácie dokumentu, pri ktorom novovzniknutý dokument má **rovnaké právne účinky** ako pôvodný.
 - Je upravená v Zákone o e-Governmente.
 - **Typy transformácie:**
 1. Z listinnej podoby do elektronickej (skenovanie).
 2. Z elektronickej podoby do listinnej (tlač).
 - **Kto ju vykonáva:** Len zákonom určené oprávnené osoby – orgány verejnej moci, notári, advokáti a **IOMO** (napr. pracoviská na poštách).
 - Súčasťou je **osvedčovacia doložka**, ktorá je autorizovaná KEP-om alebo KEPe a časovou pečiatkou.
-

OCHRANA OSOBNÝCH ÚDAJOV (GDPR)

- Kvalifikované certifikáty nevyhnutne **obsahujú osobné údaje** (meno, priezvisko, prípadne rodné číslo alebo číslo dokladu).
- Z tohto dôvodu sú kvalifikovaní poskytovatelia dôveryhodných služieb v pozícii **prevádzkovateľov osobných údajov** a musia v plnom rozsahu dodržiavať nariadenie **GDPR**.
- To zahŕňa povinnosť chrániť údaje pred zneužitím a rešpektovať práva dotknutých osôb (právo na prístup, opravu, atď.).
- Existuje napätie medzi potrebou jednoznačnej identifikácie a princípom **minimalizácie údajov** podľa GDPR.

BUDÚCNOSŤ DIGITÁLNEJ IDENTITY: EIDAS 2.0

- Najnovší krok vo vývoji je revízia nariadenia, známa ako **eIDAS 2.0 (Nariadenie (EÚ) 2024/1183)**, ktorá vstúpila do platnosti v máji 2024.
- Hlavnou inováciou je zavedenie **Európskej peňaženky digitálnej identity (EUDI Wallet)**.
- Ide o koncept **mobilnej aplikácie**, ktorú budú musieť členské štáty EÚ bezplatne poskytnúť svojim občanom a podnikom najneskôr do roku 2026.
- Predstavuje posun od modelu viazaného na fyzickú kartu (eID) k **decentralizovanému a na používateľa zameranému prístupu**.

EURÓPSKA PEŇAŽENKA DIGITÁLNEJ IDENTITY (EUDI)

EUDI Wallet umožní bezpečne uchovávať a spravovať digitálne verzie dokladov a osvedčení.

Kľúčové princípy:

- **Kontrola používateľa:** Používateľ bude mať plnú kontrolu nad svojimi dátami a rozhodne, ktoré informácie komu poskytne.
- **Selektívne zverejnenie:** Namiesto celého dokladu bude možné preukázať len jeden údaj. Napr. pri kúpe alkoholu aplikácia len potvrdí "Áno, osoba je staršia ako 18 rokov," bez odhalenia ostatných údajov.
- **Cezhraničná interoperabilita:** Peňaženka bude plne uznávaná v celej EÚ pri prístupe k verejným aj súkromným službám (otvorenie účtu v banke, check-in v hoteli).

ZHRNUTIE KLÚČOVÝCH BODOV

- **KEP** je právne rovnocenný vlastnoručnému podpisu v celej EÚ.
- **Časová pečiatka** je nevyhnutná pre dlhodobú právnu preukázateľnosť a archiváciu (LTV).
- **Mandátny certifikát** slúži na preukázanie konania v mene iného subjektu.
- **Elektronická pečat' (KEPe)** slúži na preukázanie pôvodu a integrity dokumentu od organizácie.
- Správna voľba medzi mandátnym certifikátom a pečat'ou závisí od požiadaviek zákona.
- Budúcnosť je v **mobilnej Európskej peňaženke digitálnej identity (EUDI)**, ktorá prinesie väčšiu kontrolu používateľom.

HROZBA "HARVEST NOW, DECRYPT LATER"

Prečo je kvantová hrozba akútna už dnes?

- **Scenár:** Útočník dnes zaznamenáva a ukladá vašu zašifrovanú komunikáciu.
- **Cieľ:** Dešifrovať ju v budúcnosti, keď bude mať k dispozícii kvantový počítač.
- **Dôsledok:** Dáta, ktoré musia zostať tajné mnoho rokov (vládne tajomstvá, duševné vlastníctvo, obchodné tajomstvá), sú **ohrozené už teraz**.

Prechod na kvantovo odolnú kryptografiu je naliehavý.

ĎAKUJEM ZA POZORNOST

- Otázky a odpovědi