Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

AUTENTIFIKÁCIA A AUTORIZÁCIA V DIGITÁLNOM ŠTÁTE

Kongres ITAPA, November 2022

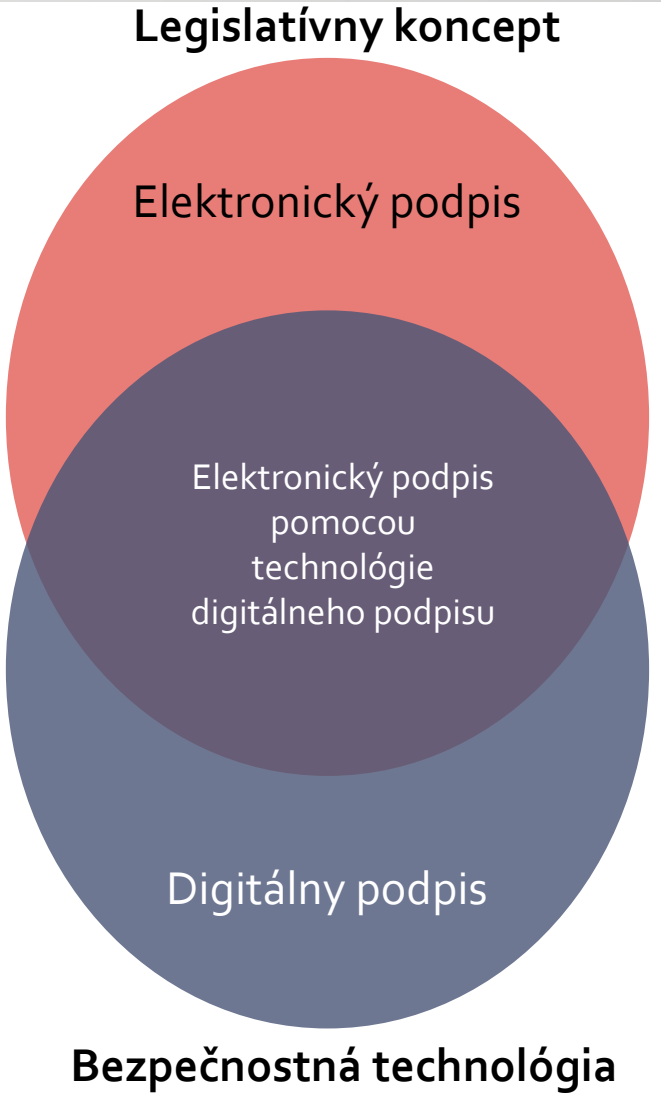
NCC-SK
SLOVAKIA CYBERSECURITY
COORDINATION CENTRE

AUTORIZÁCIA PRÁVNYCH ÚKONOV

- **Právny úkon** - je prejav vôle smerujúci najmä k vzniku, zmene alebo zániku práv alebo povinností, ktoré právne predpisy s takýmto prejavom spájajú
- **Doručenie písomnosti -** je nevyhnutným predpokladom na to, aby písomnosť spôsobila právne účinky
  - **„Písomný právny úkon je platný, len ak je PODPÍSANÝ konajúcou osobou" (**§ 40 ods. 3 OZ)
  - **„Prejav vôle pôsobí voči neprítomnej osobe od okamihu, keď jej dôjde**" (§ 45 ods. 1 OZ)
- **Podpis konajúcej osoby** je výslovným prejavom jej vôle, smerujúci ku vzniku, zmene alebo zániku práv alebo povinností
  - **Podpisom** konajúca osoba deklaruje, že je s nejakým právnym úkonom vôľovo a obsahovo stotožnená
- **Elektronický podpis** - sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie (čl. 3 ods. 10 eIDAS)

DIGITÁLNY PODPIS

- Digitálny podpis závisí nielen na podpise, ale aj na podpisovanom dokumente
- Ciele použitia digitálneho podpisu:
  - **Autenticita** – t. j. overenie totožnosti používateľa a zistenie, či deklarovaná identita používateľa je skutočná a pravá
  - **Integrita** – t. j. zaručenie, že po podpísaní digitálneho dokumentu už nedošlo k žiadnej zmene jeho obsahu
  - **Nepopierateľnosť („non-repudiation“)** – t. j. zaručenie, že právny úkon bol skutočne vedome vykonaný konajúcou osobou a že táto nebude môcť dodatočne poprieť svoj výslovný prejav vôle, vykonaný podpisom elektronického dokumentu



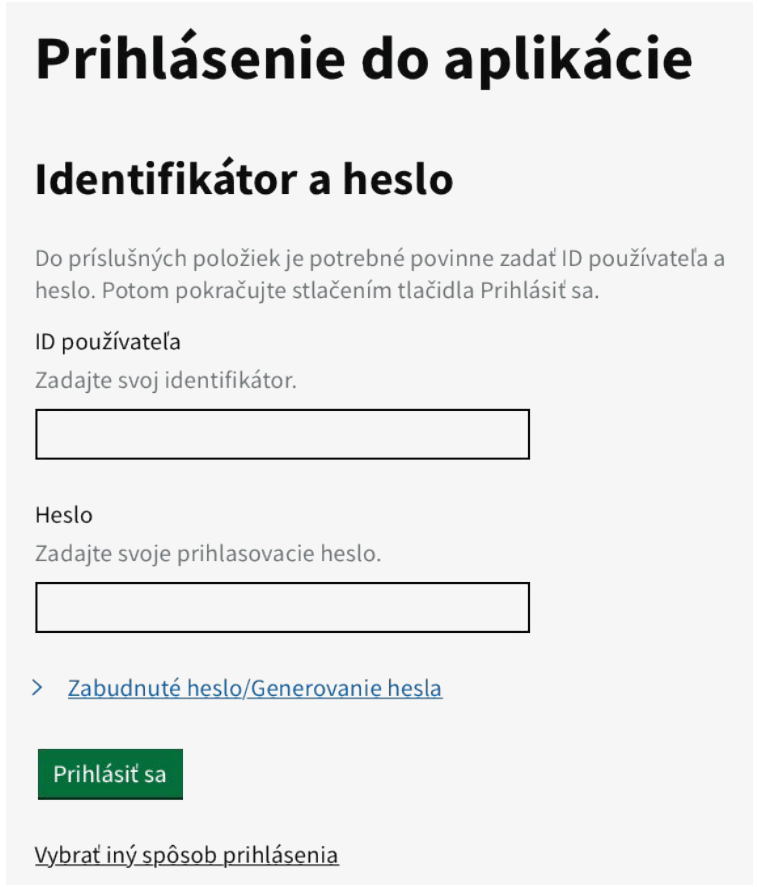
Spolufinancovaný Európskou úniou

IDENTIFIKÁCIA / AUTENTIZÁCIA / AUTORIZÁCIA

- **Identifikácia** je proces používania osobných identifikačných údajov v elektronickej forme, ktoré jedinečne reprezentujú fyzickú osobu alebo právnickú osobu (č. 3 ods. 1 eIDAS)

- **Autentizácia** je elektronický proces, ktorý umožňuje potvrdiť elektronickú identifikáciu fyzickej osoby alebo právnickej osoby alebo pôvod a integritu údajov v elektronickej forme

- **Validácia** je proces overenia a potvrdenia, že elektronický podpis alebo elektronická pečať sú platné
- **Autorizácia**, je pridelenie príslušných oprávnení na vykonanie transakcie resp. úkonu nasleduje vždy až po úspešnej autentizácii



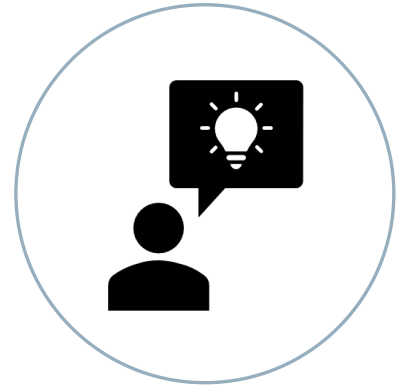
- **Autorizácia** vždy využíva výsledky **autentizácie** na pridelenie príslušných oprávnení

Spolufinancovaný Európskou úniou

OVERENIE DIGITÁLNEJ TOTOŽNOSTI

Tri základné autentizačné metódy:

1. **Niečo viem** (PIN, heslo, frázu, kód, jednorazové heslo)
2. **Niečo mám** (mobil, identifikačnú kartu, identifikačný dokument, GRID kartu, platobnú kartu, kľúč, token, čipovú kartu, RFID kartu, kartičku s QR kódom)
3. **Niečím som** (biometrický údaj - napr. odtlačok prsta, scan sietnice)



Moderné autentifikačné systémy používajú aj ďalšie metódy, napr.:

4. **Niekde som** (GPS lokalizačný údaj, IP adresa, WiFi SSID)
5. **Niečo robím** (tzv. behaviorálny údaj, kontext konania)

Každá z metód autentizácie má v konkrétnom použití svoje výhody a nevýhody, často sa metódy v praxi kombinujú (najmä v MFA)

Spolufinancovaný Európskou úniou

AUTENTIZAČNÉ / AUTORIZAČNÉ PRVKY

Statické tajné informácie

- Autentizačný údaj predstavuje statická informácia (slovo, číslo, kód, fráza...)

Jednorazové tajné informácie

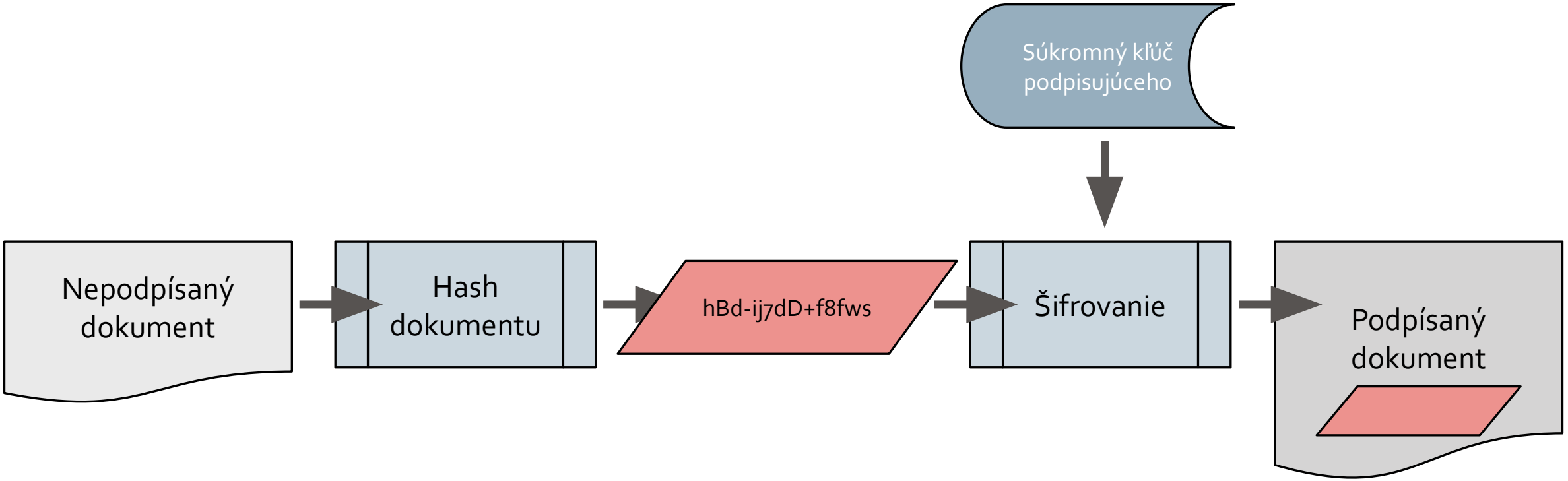
- Autentizačný údaj je pri každom prístupe do systému dynamicky generovaný; zvyčajne má aj obmedzenú časovú platnosť

Kryptografické algoritmy

- Predovšetkým metóda súkromného a verejného kľúča

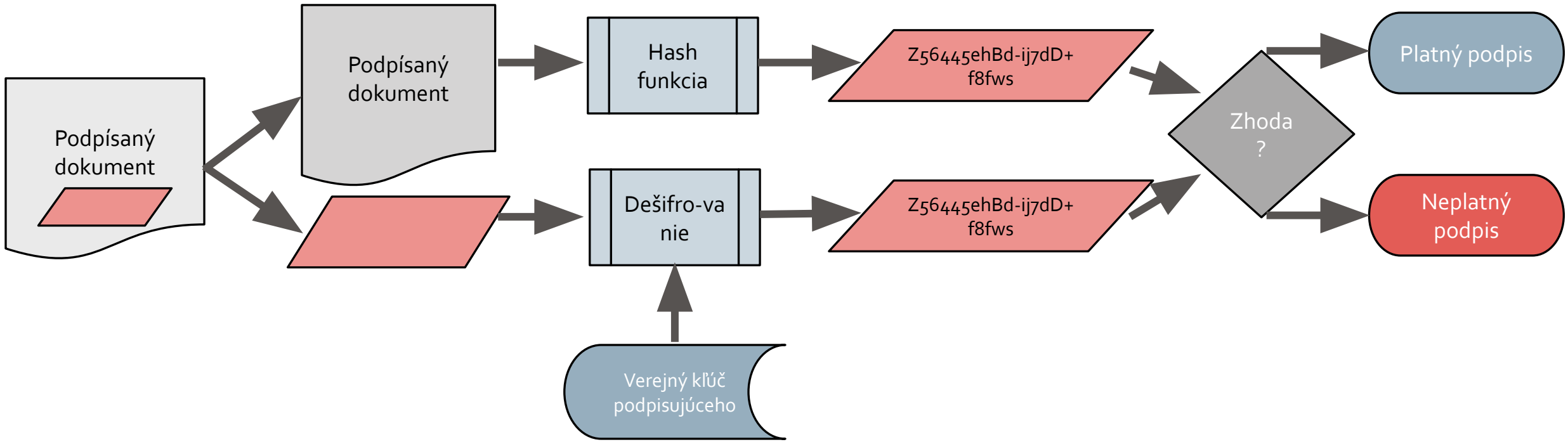
Spolufinancovaný Európskou úniou

VYTVORENIE DIGITÁLNEHO PODPISU



Spolufinancovaný Európskou úniou

OVERENIE DIGITÁLNEHO PODPISU



Spolufinancovaný Európskou úniou

STUPNE DÔVERYHODNOSTI DIGITÁLNEJ IDENTIFIKÁCIE PODĽA eIDAS

Pre prostriedky elektronickej identifikácie eIDAS špecifikuje úrovne zabezpečenia:

- **obmedzený stupeň dôveryhodnosti**, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, charakterizovaný odkazom na technické špecifikácie, normy a postupy, ktorých účelom je **znížiť riziko zneužitia alebo pozmenenia totožnosti**

- **pokročilý stupeň dôveryhodnosti**, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, charakterizovaný odkazom na technické špecifikácie, normy a postupy, ktorých účelom je **podstatne znížiť riziko zneužitia alebo pozmenenia totožnosti**

- **vyšší stupeň dôveryhodnosti**, ako prostriedok elektronickej identifikácie s úrovňou zabezpečenia „**pokročilá**“, pokiaľ ide o údajnú alebo uvádzanú totožnosť osoby, charakterizovaný odkazom na technické špecifikácie, normy a postupy, ktorých účelom je **zabrániť zneužitiu alebo pozmeneniu totožnosti**

MOŽNÉ ÚROVNE DÔVERYHODNOSTI DIGITÁLNEJ IDENTIFIKÁCIE

Navrhovaný názov úrovne	Metóda digitálnej identifikácie	Nespochybni-teľnosť úkonu	Dôveryhod-nosť identifikácie konajúcej osoby	Integrita dokumentu	Časová pečiatka	QSCD	Úroveň zabezpečenia podľa eIDAS
Osvedčená	KEP + časová pečiatka	Áno	Vysoká	Áno	Áno	Áno	vyššia
Kvalifikovaná	KEP	Áno	Vysoká	Áno	Nie	Áno	vyššia
Zdokonalená	AdES	Áno	Vysoká	Áno	Nie	Áno	pokročilá
Stredná	EP	Nie	Pokročilá	Áno	Nie	Nie	obmedzená
Nízka	Proprietárne riešenia	Nie	Nízka	Áno	Nie	Nie	obmedzená

Spolufinancovaný Európskou úniou

PRÁVNE ÚČINKY JEDNOTLIVÝCH METÓD DIGITÁLNEJ IDENTIFIKÁCIE

Metóda	Právny účinok / Typický spôsob použitia
KEP + časová pečiatka	právne úkony, pre ktoré **je požadované** osvedčenie podpisu
KEP	právne úkony, pre ktoré je vyžadovaný vlastnoručný podpis, avšak **nie je požadované** osvedčenie podpisu
Zdokonalený elektronický podpis	dôveryhodné určenie totožnosti konajúcej osoby pre výslovný prejav vôle
"Obyčajný" elektronický podpis	nepriame určenie totožnosti osoby v uzatvorenom systéme
Proprietárne riešenia	autorizácia právneho úkonu v uzatvorenom systéme

Spolufinancovaný Európskou úniou

OTVORENÉ OTÁZKY

- Aké metódy digitálnej identifikácie sú / budú prípustné v ISVS?
- Ako vnímajú gestori právnych predpisov rovnocennosť výslovného prejavu vôle vo fyzickom svete a v kybernetickom priestore?
- Do akej miery sa ISVS/eGov zaoberajú otázkami elektronického doručovania?
- Ako by mal štát riešiť otázky účinnosti elektronického doručovania?
- Sú proprietárne metódy identifikácie dostatočne dôveryhodné pre výslovný prejav vôle v právnych vzťahoch so štátom?
- Ako zjednodušenie foriem autorizácie súvisí s konceptom Open data?
- Je vo všeobecnosti prípustný odklon od kryptografických metód identifikácie a autorizácie?
- Ktoré metódy autorizácie by mohli byť použité pre menej závažné právne úkony?
- Pre ktoré právne úkony budú akceptovateľné proprietárne metódy identifikácie a autorizácie?
- Kto by mal rozhodnúť o zrovnoprávnení foriem autorizácie vo fyzickom a virtuálnom svete?
- Aké by mali byť ďalšie kroky v konsolidácii metód digitálnej identifikácie, autorizácie a doručovania pre potreby ISVS?

PANELOVÁ DISKUSIA

- Radovan Ako, CRIF – Slovak Credit Bureau
- Ján Bučkuliak, Úrad vlády SR
- Pavol Frič, DITEC
- Patrik Plachý, RED HAT
- Ľubomír Illek, Slovensko.digital

Spolufinancovaný Európskou úniou

Spolufinancovaný Európskou úniou

Ochrana vlastníckych práv

Vlastnícke práva tretích strán

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.