



MINISTERSTVO
VNÚTRA
SLOVENSKEJ REPUBLIKY

**Integračná príručka
pre špecializovaný technický produkt**

**Rozhranie aplikácie eIDENTITA pre integráciu na
funkcionalitu vyhotovenia elektronického podpisu s
využitím KEP na eID alebo eDoPP**

Verzia dokumentu:

5.3.2026, verzia 1.1

Obsah

ROZHRAVIE APLIKÁCIE EIDENTITA PRE INTEGRÁCIU NA FUNKCIONALITU VYHOTOVENIA ELEKTRONICKÉHO PODPISU S VYUŽITÍM KEP NA EID ALEBO EDOPP	1
OBSAH	2
1 ÚVOD	3
1.1 IDENTIFIKÁCIA A URČENIE	3
1.2 ZMENOVÝ LIST	3
1.3 DEFINÍCIA POJMOV A SKRATIEK	4
1.4 REFERENCIE	5
1.5 ZOZNAM OBRÁZKOV	6
1.6 ZOZNAM TABULIEK	6
2 ROZSAH PLATNOSTI A ÚČEL	7
3 SCENÁRE INTEGRÁCIE V PROSTREDÍ ONLINE APLIKÁCIÍ	8
3.1 PODPÍSANIE DOKUMENTU Z WEBOVEJ APLIKÁCIE NA POČÍTAČI (DESKTOP2MOBILE)	9
3.2 PODPÍSANIE DOKUMENTU Z WEBOVEJ APLIKÁCIE V MOBILNOM ZARIADENÍ (WEB2APP)	10
3.3 PODPÍSANIE DOKUMENTU Z NATÍVNEJ APLIKÁCIE V MOBILE (APP2APP)	11
3.4 FORMÁTY DEEPLINKOV A QR KÓDOV	12
3.4.1 <i>Formát so všetkými parametrami v deeplinku / QR</i>	13
3.4.2 <i>Formát s odkazom na JSON</i>	15
4 SCENÁR INTEGRÁCIE S LOKÁLNYM ODOVZDANÍM SÚBORU NA PODPIS	16

1 ÚVOD

1.1 IDENTIFIKÁCIA A URČENIE

Tento dokument obsahuje technickú špecifikáciu rozhrania, prostredníctvom ktorého mobilná aplikácia eIDENTITA poskytuje integrujúcim sa systémom / aplikáciám funkcionality **autorizácie dokumentov vyhotovením kvalifikovaného elektronického podpisu (KEP)** s využitím kvalifikovaného certifikátu uloženého v čipe **občianskeho preukazu (eID)** alebo **preukazu povolenia na pobyt (eDoPP)**.

Dokument je určený pre vývojárov webových alebo mobilných aplikácií, ktorí plánujú do svojich riešení integrovať autorizáciu prostredníctvom vyššie menovanej funkcionality aplikácie eIDENTITA.

1.2 ZMENOVÝ LIST

Verzia	Dátum	Autor	Dôvod zmeny	Kapitola, Bod
1.0	24.11.2025	MV SR	Iniciálna verzia	
1.1	05.03.2026	MV SR	Upresnenie popisu parametra destinationUrl	Kap. 3.4, Tabuľka 2

1.3 DEFINÍCIA POJMOV A SKRATIEK

Skratka / pojem	Vysvetlenie
BOK	Bezpečnostný osobný kód
eID	Elektronická identifikačná karta (občiansky preukaz s čipom)
eDoPP	Elektronický doklad Povolenie na pobyt
EK	Európska komisia
KEP	Kvalifikovaný elektronický podpis
MeID	Mobilné eID
mSDK	Mobilné SDK
MV SR	Ministerstvo vnútra Slovenskej republiky
QES	Qualified Electronic Signature
QSCD	Qualified Signature Creation Device (kvalifikované zariadenie pre vyhotovenie elektronického podpisu)
SCA	Signature Creation Application
SDK	Software Development Kit
SP	Poskytovateľ služby, za angl. Service Provider

1.4 REFERENCIE

- [1] Aplikácia eIDENTITA - Používateľská príručka
- [2] Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

1.5 ZOZNAM OBRÁZKOV

Obrázok 1: Podpis desktop2mobile	9
Obrázok 2: Podpis web2app.....	10
Obrázok 3: Podpis app2app	11
Obrázok 3: Podpis share2app.....	16

1.6 ZOZNAM TABULIEK

Tabuľka 1: Custom URL schéma pre podpisovanie	12
Tabuľka 2: Vstupné parametre na podpis	12
Tabuľka 3: Riadiace parametre podpisu.....	13

2 ROZSAH PLATNOSTI A ÚČEL

Tento dokument slúži ako integračná príručka pre tvorcov technických riešení, ktorí do svojich riešení plánujú **integrovat' autorizáciu dokumentov s využitím kvalifikovaného elektronického podpisu (KEP)** vyhotoveného prostredníctvom kvalifikovaného certifikátu uloženého v čipe eID resp. eDoPP, pričom na tento účel plánujú **využiť funkcionality poskytovanú aplikáciou eIDENTITA.**

Jednou z funkcionalít, ktoré Aplikácia eIDENTITA poskytuje, je funkcionality **Aplikácie pre vyhotovenie elektronického podpisu** (z angl. Signature Creation application). Aplikácia umožňuje vytvorenie kvalifikovaného elektronického podpisu vo formátoch:

- **PAdES** – formát vhodný pre podpisovanie PDF dokumentov,
- **ASiC-E XAdES** – formát vhodný pre podpisovanie širšej množiny formátov:
 - aktuálne podporované formáty podpisovaných súborov akceptované v komunikácii s orgánmi verejnej moci : PDF, TXT, PNG a ASiC-E,
 - pripravované formáty podpisovaných súborov pre komunikáciu s orgánmi verejnej moci: XML (elektronické formuláre)
 - iné formáty, ktoré v komunikácii s orgánmi verejnej moci nemusia byť akceptované, avšak môžu byť použité v súkromnej alebo komerčnej komunikácii: napr. JPG, JPEG, HEiC, DocX, XLSX a ďalšie.

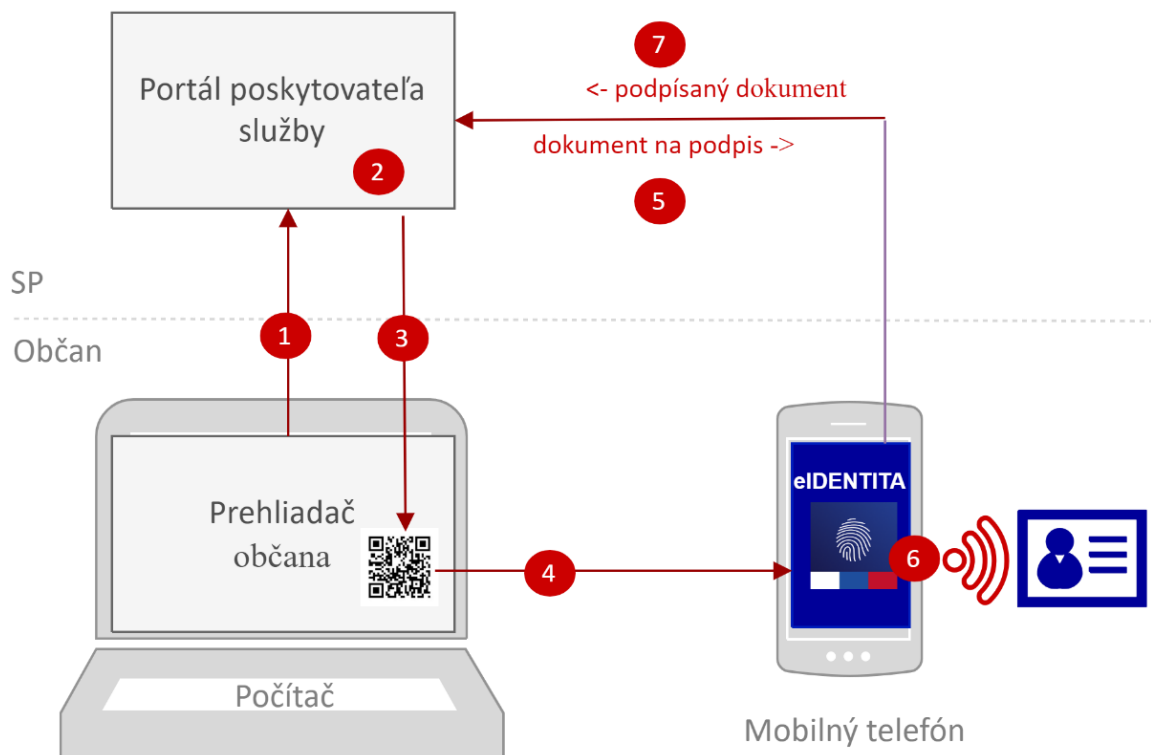
S cieľom podporiť širšie využívanie **eID** v digitálnych službách verejného aj súkromného sektora, ponúka aplikácia **eIDENTITA** svoju funkcionality prostredníctvom **otvoreného a jednoducho integrovateľného technického rozhrania.**

3 SCENÁRE INTEGRÁCIE V PROSTREDÍ ONLINE APLIKÁCIÍ

Aplikácie eIDENTITA poskytuje technické rozhranie pre umožnenie integrácie podpisovania z prostredia webových a mobilných aplikácií, pričom sú podporované nasledovné režimy interakcie:

- podpisovanie v režimoch **desktop2mobile** a **web2app** umožní podpísať súbor v rámci webovej aplikácie poskytovateľa služby bežiacej v prehliadači v mobile alebo na desktpe, pričom aplikácia eIDENTITA je aktivovaná cez deep linku resp. QR kód. V parametroch deep linky resp. QR kódu je definovaná URL na dokument, ktorý má byť podpísaný a tiež URL, na ktorú má byť odoslaný podpísaný dokument. eIDENTITA si z definovanej URL stiahne dokument na podpis, v interakcii s používateľom vyhotoví KEP a výsledný podpísaný dokument odošle na definovanú URL,
- podpisovanie v režime **app2app** s online výmenou súborov umožní podpísať súbor v rámci natívnej aplikácie poskytovateľa služby bežiacej v mobilnom zariadení, pričom aplikácia eIDENTITA je aktivovaná cez deep linku. V parametroch deep linky je definovaná URL na dokument, ktorý má byť podpísaný a tiež URL, na ktorú má byť odoslaný podpísaný dokument. eIDENTITA si z definovanej URL stiahne dokument na podpis, v interakcii s používateľom vyhotoví KEP a výsledný podpísaný dokument odošle na definovanú URL.

3.1 PODPÍSANIE DOKUMENTU Z WEBOVEJ APLIKÁCIE NA POČÍTAČI (DESKTOP2MOBILE)

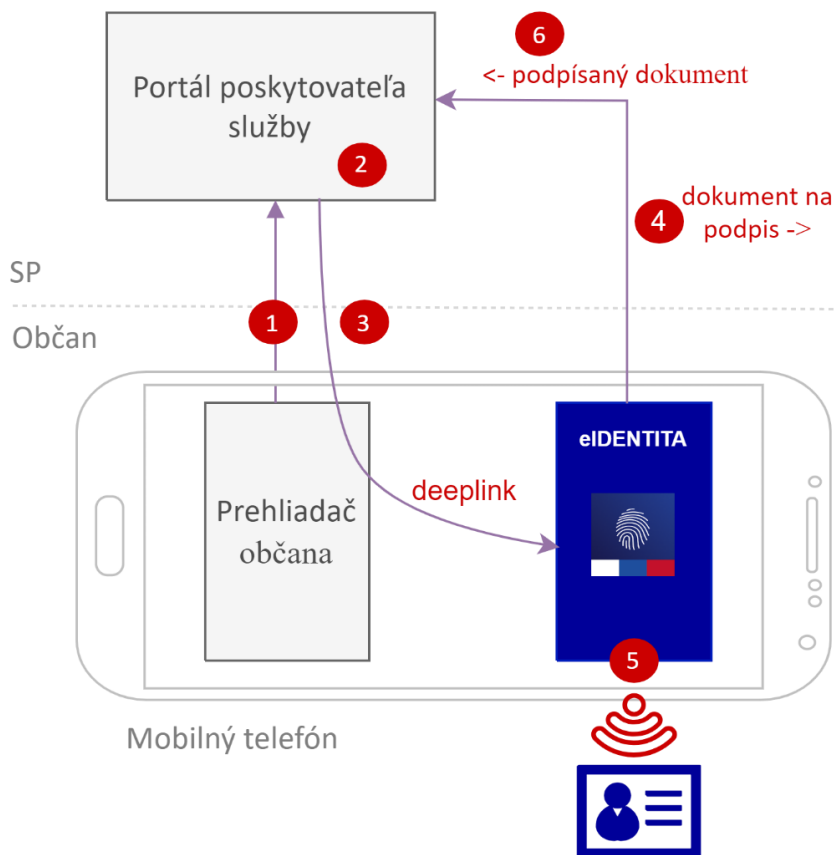


Obrázok 1: Podpis desktop2mobile

1. Upload dokumentu na podpísanie alebo vyplnenie formulára
2. Sprístupnenie dokumentu na podpis
3. Vygenerovanie QR kódu
4. Spustenie eIDENTITA a naskenovanie QR kódu
5. Automatické stiahnutie dokumentu na podpis
6. Vyhotovenie KEP
 - a. Zobrazenie dokumentu
 - b. Voľba „Podpísať“
 - c. Zadanie BOK a KEP PIN
 - d. Vytvorenie podpisu vo formáte EÚ
7. Upload podpísaného dokumentu

Pozn.: QR kód (bod 3) vo svojich parametroch obsahuje adresu dokumentu na podpis a adresu pre spätné nahranie podpísaného dokumentu

3.2 PODPÍSANIE DOKUMENTU Z WEBOVEJ APLIKÁCIE V MOBILNOM ZARIADENÍ (WEB2APP)

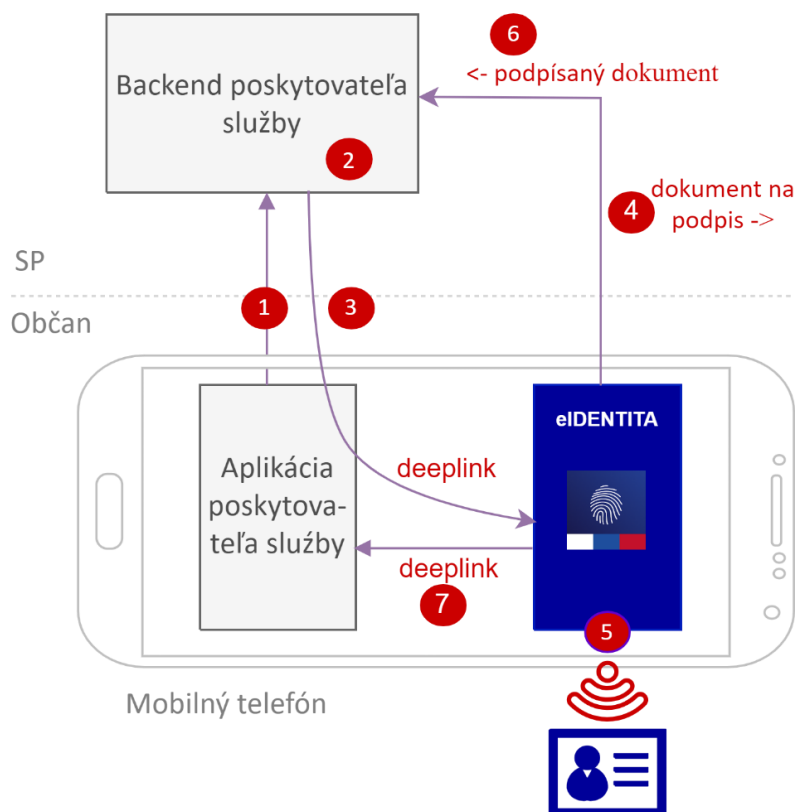


Obrázok 2: Podpis web2app

1. Upload dokumentu na podpísanie alebo vyplnenie formulára
2. Sprístupnenie dokumentu na podpis
3. Spustenie eIDENTITA
4. Automatické stiahnutie dokumentu na podpis
5. Vyhotovenie KEP
 - a. Zobrazenie dokumentu
 - b. Voľba „Podpísať“
 - c. Zadanie BOK a KEP PIN
 - d. Vytvorenie podpisu vo formáte EÚ
6. Upload podpísaného dokumentu

Pozn.: Deep link (bod 3) vo svojich parametroch obsahuje adresu dokumentu na podpis a adresu pre spätné nahratie podpísaného dokumentu (rovnako ako QR pri Desktop2Mobile)

3.3 PODPÍSANIE DOKUMENTU Z NATÍVNEJ APLIKÁCIE V MOBILE (APP2APP)



Obrázok 3: Podpis app2app

1. Upload dokumentu na podpísanie alebo vyplnenie formulára
2. Sprístupnenie dokumentu na podpis
3. Spustenie eIDENTITA
4. Automatické stiahnutie dokumentu na podpis
5. Vyhotovenie KEP
 - a. Zobrazenie dokumentu
 - b. Voľba „Podpísať“
 - c. Zadanie BOK a KEP PIN
 - d. Vytvorenie podpisu vo formáte EÚ
6. Upload podpísaného dokumentu
7. Vrátenie riadenia do volajúcej aplikácie

Pozn.: Deep link (bod 3) vo svojich parametroch obsahuje adresu dokumentu na podpis a adresu pre spätné nahratie podpísaného dokumentu (rovnako ako QR pri Desktop2Mobile), ako aj call back URL pre vrátenie riadenia do volajúcej aplikácie.

3.4 FORMÁTY DEEPLINKOV A QR KÓDOV

Pre integráciu podpisovej funkcionality je použitá nasledovná custom URL schéma:

Tabuľka 1: Custom URL schéma pre podpisovanie

Schéma	Prostredie
sk.minv.sca://sign	MV PROD

Parametre pre podpisovú operáciu:

Tabuľka 2: Vstupné parametre na podpis

Parameter	Popis	Povinný
sourceUrl	string, url odkiaľ si má eIDENTITA stiahnuť dokument na podpis. Za bezpečnosť URL (napr. zabezpečenie náhodne generovaným stringom v kontextovej ceste, limitovaná doba platnosti) je zodpovedný integrátor.	Áno
destinationUrl	string, url kam má byť uploadnutý podpísaný dokument. Ak nie je uvedený, aplikácia neuploadne podpísaný súbor, používateľ ho má možnosť len vyzdieľať štandardným spôsobom. Za bezpečnosť URL (napr. zabezpečenie náhodne generovaným stringom v kontextovej ceste, limitovaná doba platnosti) je zodpovedný integrátor. Odoslanie sa vykoná pomocou HTTP POST požiadavky s typom obsahu multipart/form-data.	Nie
callbackUrl	string, url (deeplink), ktorú aplikácia zavolá po úspešnom podpise. Ak nie je uvedený, používateľ nie je presmerovaný naspäť do pôvodnej aplikácie, resp. zostane v eIDENTITE na podpísanom dokumente a má možnosť podpísaný dokument štandardne vyzdieľať.	Nie
signatureFormat	string, " pades " alebo " asice-xades ". Ak nie je uvedený, bude zvolený defaultný typ podpisu. Pre PDF súbory PAdES, pre ostatné typy súborov ASiC-E XAdES.	Nie
signatureType	string, " certified " alebo " handwritten ", kde „ certified “, znamená že bude vytvorený kvalifikovaný elektronický podpis s časovou pečiatkou rovnocenný úradne osvedčenému podpisu v zmysle § 23, ods. (1), bod b) zákona 305/2013 Z.z. (zákon o eGovernmente). „ handwritten “, znamená že bude vytvorený kvalifikovaný elektronický podpis bez časovej pečiatky rovnocenný vlastnoručnému podpisu v zmysle § 23, ods. (1), bod a) zákona 305/2013 Z.z. (zákon o eGovernmente).	Nie

	Ak parameter nie je uvedený, aplikácia sa spýta používateľa, aký typ podpisu si želá vytvoriť.	
--	--	--

Uvedené parametre môžu byť uvedené priamo v deppelinku alebo v dátovej štruktúre JSON, ktorý si aplikácia eIDENTITA stiahne z URL definovanej v parametri **linkURL**, ako je uvedené nižšie.

Riadiace parametre:

Tabuľka 3: Riadiace parametre podpisu

Parameter	Popis	Povinný
linkURL	string, url odkiaľ si má eIDENTITA stiahnuť JSON s parametrami definovanými v tabuľke vyššie. Použije sa v prípade, že integrujúca s aplikácia preferuje definíciu vstupných parametrov cez JSON.	Nie
qr	Informácia, či je operácia iniciovaná QR kódom.	Nie

3.4.1 Formát so všetkými parametrami v deeplinku / QR

V tomto prípade sú všetky vstupné parametre definované v deeplinku, príklad:

sk.minv.sca://sign?sourceUrl=https%3A%2F%2Fdemo-storage.eid.minv.sk%2Fapi%2Fdocument%2F3cb7d764-343f-4bae-8fd6-c313651e074f%2Fdownload&destinationUrl=https%3A%2F%2Fdemo-storage.eid.minv.sk%2Fapi%2Fdocument%2Fupload%2Fcafa3711-b1f5-45c6-920d-827a6a91314c&callbackUrl=https%3A%2F%2Fdemo-portal.eid.minv.sk%2Fsign-application%3Fresponse_id%3Dcafa3711-b1f5-45c6-920d-827a6a91314c&qr=true&signatureFormat=asice-xades&signatureType=certified

Príklad zobrazenia deeplinku v QR kóde:



3.4.2 Formát s odkazom na JSON

V tomto prípade je v deeplinku uvedená URL na JSON, ktorý obsahuje všetky vstupné parametre, príklad:

sk.minv.sca://sign?qr=true&linkUrl=https%3A%2F%2Fdemo-storage.eid.minv.sk%2Fapi%2Fdocument%2FgetJsonInfo%2F3cb7d764-343f-4bae-8fd6-c313651e074f

Príklad zobrazenia deeplinku v QR kóde:



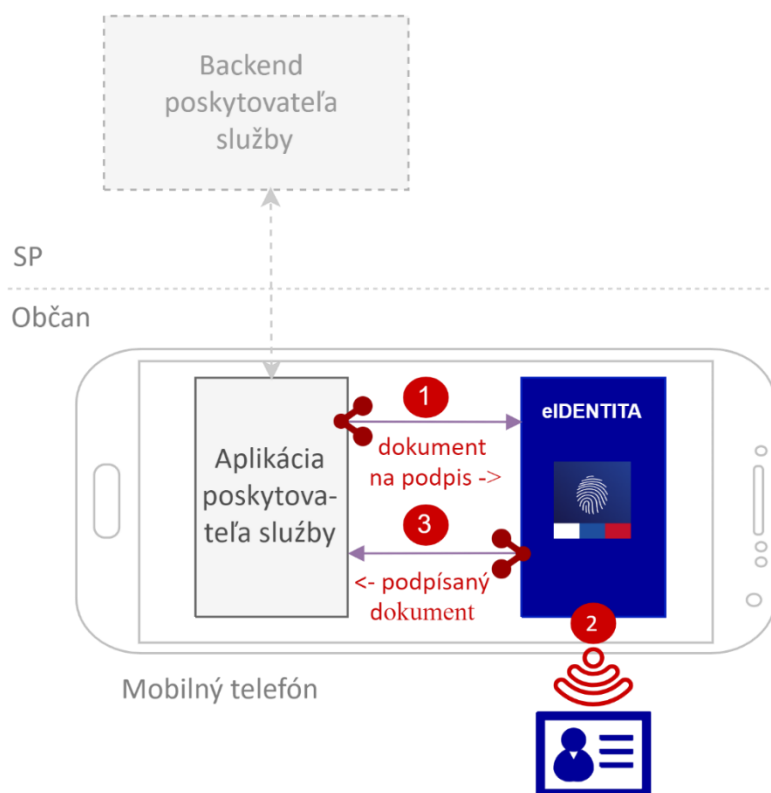
Príklad JSON po stiahnutí z linkURL:

```
{  
  "sourceUrl": "https://demo-storage.eid.minv.sk/api/document/3cb7d764-343f-4bae-8fd6-c313651e074f/download",  
  "signatureFormat": "asice-xades",  
  "signatureType": "certified",  
  "callbackUrl": "https://demo-portal.eid.minv.sk/sign-application?response_id=cafa3711-b1f5-45c6-920d-827a6a91314c",  
  "destinationUrl": "https://demo-storage.eid.minv.sk/api/document/upload/cafa3711-b1f5-45c6-920d-827a6a91314c"  
}
```

4 SCENÁR INTEGRÁCIE S LOKÁLNYM ODOVZDANÍM SÚBORU NA PODPIS

Okrem integrácie prostredníctvom deep linku (v prípade ktorého prebieha výmena dokumentov online spôsobom) je možné podpísanie dokumentu v aplikácii eIDENTITA iniciovať aj odoslaním **lokálneho dokumentu** cez štandardnú funkcionality zdieľania (share) v rámci operačného systému mobilného zariadenia.

Priebeh podpísania lokálneho súboru s iniciovaním podpísania cez share extension je znázornený na nasledovnom obrázku:



Obrázok 4: Podpis share2app

1. Odovzdanie dokumentu na podpis cez funkciu share (user-driven – používateľ vyberá cieľovú apku)
2. Vyhotovenie KEP
 - a. Zobrazenie dokumentu
 - b. Voľba „Podpísať“
 - c. Zadanie BOK a KEP PIN
 - d. Vytvorenie podpisu vo formáte EÚ
3. Odovzdanie dokumentu späť do volajúcej aplikácie cez funkciu share (user-driven – používateľ vyberá cieľovú apku)