

Špecifikácia predmetu Zmluvy

Použité skratky

eID	- Občiansky preukaz s čipom
eDesk	- Modul elektronického doručovania ako jeden z modulov Ústredného portálu verejnej správy.
FD	- FirstData
GUID	- Globally Unique Identifier
IAM	- Identity and access management ako spoločný modul ÚPVS
IS PEP	- Centrálny systém pre evidenciu poplatkov, ktorého správcom je Ministerstvo financií Slovenskej republiky
IS VS	- Informačný systém verejnej správy
MetaIS	- Centrálny metainformačný systém verejnej správy SR, ktorý slúži pre podporu riadenia informatizácie verejnej správy a systému pre tvorbu politík v oblasti informačnej spoločnosti, ako aj pre podporu cieľov efektívnej verejnej správy, ktorými sú vytvorenie inkluzívnej informačnej spoločnosti ako prostriedku pre rozvoj vysoko výkonnej vedomostnej ekonomiky.
MEP	- Modul elektronických platieb ako jeden z modulov Ústredného portálu verejnej správy.
MF SR	- Ministerstvo financií Slovenskej republiky
PABK	- Poštová banka, a.s.
PnÚ	- Príkaz na úhradu = platobný predpis
SP, a. s.	- Slovenská pošta, a. s.
SSO	- Single Sign On (jednotné prihlasovanie)
SW	- Softvér
ÚPVS	- Ústredný portál verejnej správy
VS	- Variabilný symbol
Zb., Z. z.	- Zbierka zákonov

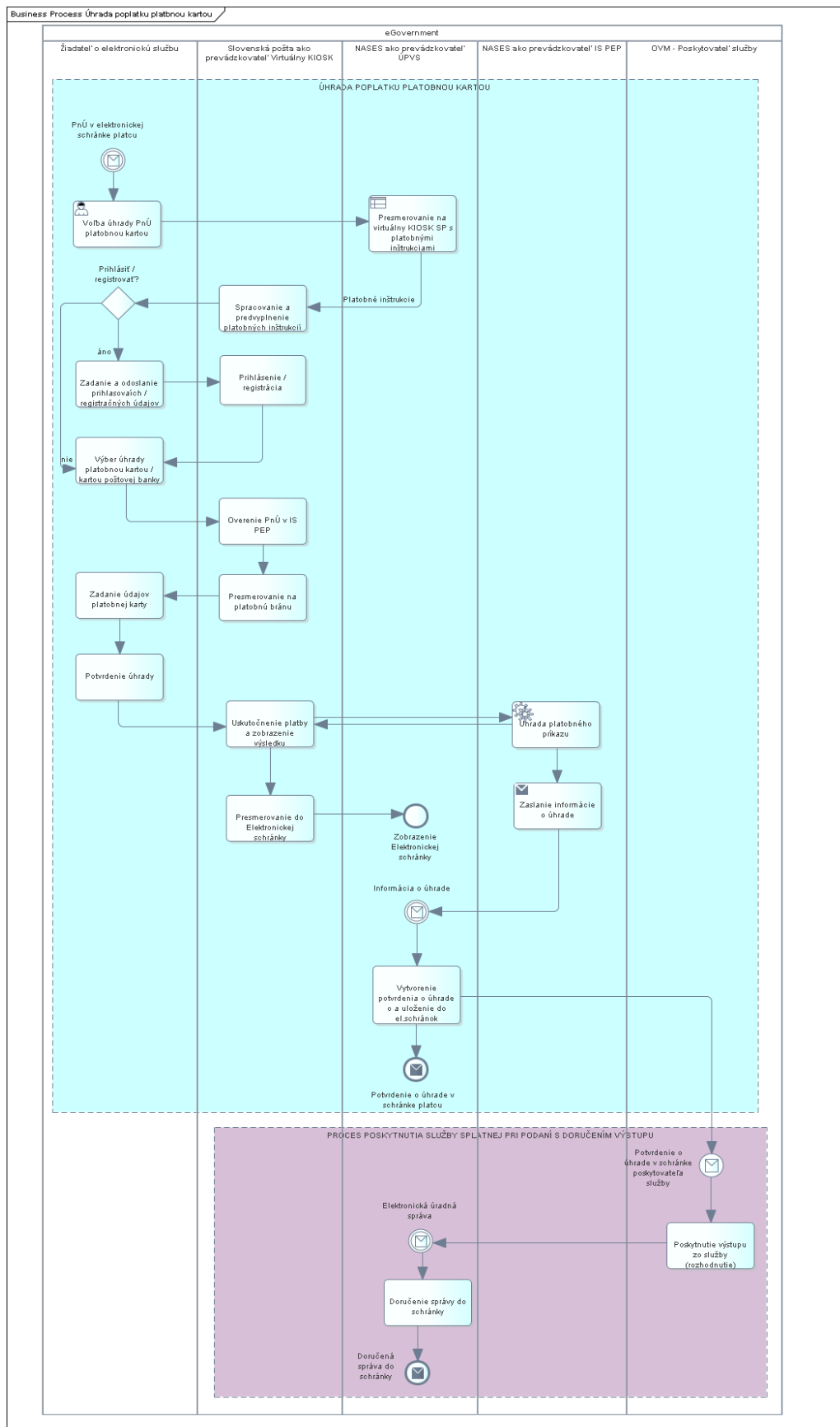
Uvedené dielo umožní implementáciu platby kartou do prostredia eGovernmentu prostredníctvom platobného kanálu, ktorý je súčasťou služby eKoloK - komplexná platobná služba štátu za služby poskytované orgánmi verejnej moci v rozsahu správnych a súdnych poplatkov podľa zákona č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov a zákona č. 71/1992 Zb. o súdnych poplatkoch a poplatku za výpis z registra trestov v znení neskorších predpisov.

Popis procesu úhrady poplatku kartou za elektronické služby na www.slovensko.sk

Po splnení predpokladov na strane poskytovateľa služby (vytvorenie PnÚ jednotným procesom) a platcu (prihlásenie do schránky), je potrebné zabezpečiť vykonanie úhrady poplatku z prostredia elektronickej schránky na www.slovensko.sk nižšie uvedeným procesom. Pre lepšiu ilustráciu je znázornený aj proces poskytnutia elektronickej služby po úspešnej úhrade poplatku.

Diagram procesu úhrady poplatku platobnou kartou na www.slovensko.sk

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronické služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 1/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*



<p>Parafy:</p>	<p>Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronické služby vyžiadané cez Slovensko.sk</p>	<p>Odborný garant: Ú GRAF-SIT</p>
	<p>Strana 2/9</p>	<p>Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*</p>

Popis procesu:

1. Platca vyberie možnosť platby kartou kliknutím na tlačidlo „platba kartou“ v elektronickej schránke.
2. Presmerovanie platcu na webovú aplikáciu eKolak
 - a. eDesk zašle platobné inštrukcie z doručeného PnÚ do webovej aplikácie eKolak a návratovú adresu pre spätné presmerovanie do elektronickej schránky. Súčasťou presmerovania z eDesk na webovú aplikáciu eKolak je aj informácia o identite platcu uložená v tokene.
 - b. Prihlásenie / registrácia vo webovej aplikácii eKolak alebo preskočenie prihlásenia podľa výberu platcu (prihlásenie/registrácia je viazané na GUID z IAM a nie je možné ho zmeniť).
 - c. Webová aplikácia eKolak spracuje doručené platobné inštrukcie a predvyplní ich.
3. Overenie PnÚ vo webovej aplikácii eKolak
 - a. Webová aplikácia eKolak pošle požiadavku do IS PEP pre overenie PnÚ s identifikačnými údajmi PnÚ, na základe ktorých IS PEP vráti stav PnÚ.
 - b. Ak PnÚ nie je vo validnom stave, t. j. predpis je úplne uhradený alebo stornovaný alebo expirovaný potom:
 - i. Úhrada nie je realizovaná.
 - ii. Webová aplikácia eKolak zobrazí informáciu o nemožnosti vykonať úhradu z dôvodu nepovoleného stavu PnÚ.
 - iii. Webová aplikácia eKolak umožní presmerovať platcu späť do elektronickej schránky.
 - c. Ak PnÚ je vo validnom stave, t. j. predpis nie je vôbec uhradený alebo je uhradený čiastočne, potom:
 - i. Pokračuje sa zadaním platobných údajov z karty, pričom webová aplikácia eKolak si získa platobné údaje z PnÚ.
4. Uskutočnenie platby vo webovej aplikácii eKolak

Pri realizovaní úhrady poplatku môžu nastať nasledujúce stavy:

 - Predpis bol uhradený.
 - Úhrada bola neúspešná z dôvodu:
 - expirácie platobnej karty,
 - nedostatku finančných prostriedkov na platobnej karte,
 - nepovolenej internetovej komunikácie na platobnej karte,
 - nesprávne vyplnených údajov z platobnej karty.
 - Úhrada nebola vykonaná z dôvodu, že sa platca rozhodol úhradu nevykonať.
 - Úhrada nebola vykonaná z dôvodu, že vypršala session.
 - a. Presmerovanie do rozhrania FirstData (SKPAY)
 - i. Ak platca nezadá údaje alebo zadá a namiesto potvrdenia platby sa vráti späť do rozhrania webovej aplikácie eKolak, webová aplikácia eKolak zobrazí informáciu o nerealizovanej platbe a umožní presmerovanie platcu späť do elektronickej schránky.
 - ii. Ak platca zadá údaje a potvrdí platbu, pokračuje sa potvrdením transakcie kartovým operátorom.
 - b. Potvrdenie transakcie kartovým operátorom

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronicke služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 3/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*

- i. Ak je karta exspirovaná alebo nedisponuje dostatočným objemom finančných prostriedkov alebo nemá zrealizované nastavenia pre výkon činnosti typu eCommerce (internetové platby) alebo zadá nesprávne údaje platobnej karty, kartový operátor zašle informáciu o neúspešnej úhrade, webová aplikácia eKolok zobrazí informáciu o nezrealizovanej platbe, proces končí presmerovaním platcu späť do elektronickej schránky, prípadne platca bude mať možnosť ukončiť proces priamo vo webovej aplikácii eKolok.
 - ii. Ak sa platca na stránke zdrží dlhšie ako je nastavená dĺžka session, úhrada nie je zrealizovaná a proces skončí. Ak platca chce pokračovať v činnostiach v elektronickej schránke, musí sa v tomto prípade opäť prihlásiť na Slovensko.sk.
 - iii. Ak karta nie je exspirovaná a disponuje dostatočným objemom finančných prostriedkov, má zrealizované nastavenia pre výkon činnosti typu eCommerce a zároveň platca zadá správne údaje z platobnej karty, kartový operátor potvrdí úspešnosť transakcie, webová aplikácia eKolok zašle informáciu do IS PEP o úspešnosti úhrady a IS PEP zmení stav predpisu. Zároveň webová aplikácia eKolok zobrazí platcovi informáciu o úspešnej úhrade a umožní presmerovanie platcu späť do elektronickej schránky.
5. Webová aplikácia eKolok zaeviduje úhradu PnÚ v IS PEP a zobrazí informáciu o úspešnej úhrade PnÚ vo webovej aplikácii eKolok.
 6. Webová aplikácia eKolok umožní presmerovanie platcu do jeho elektronickej schránky.
 7. IS PEP zašle informácie o úhrade PnÚ do MEP.
 8. MEP zašle potvrdenie o úhrade PnÚ do elektronickej schránky platcu a poskytovateľa služby.
 9. Poskytovateľ služby poskytne elektronickú službu (platí pre služby splatné pri podaní).

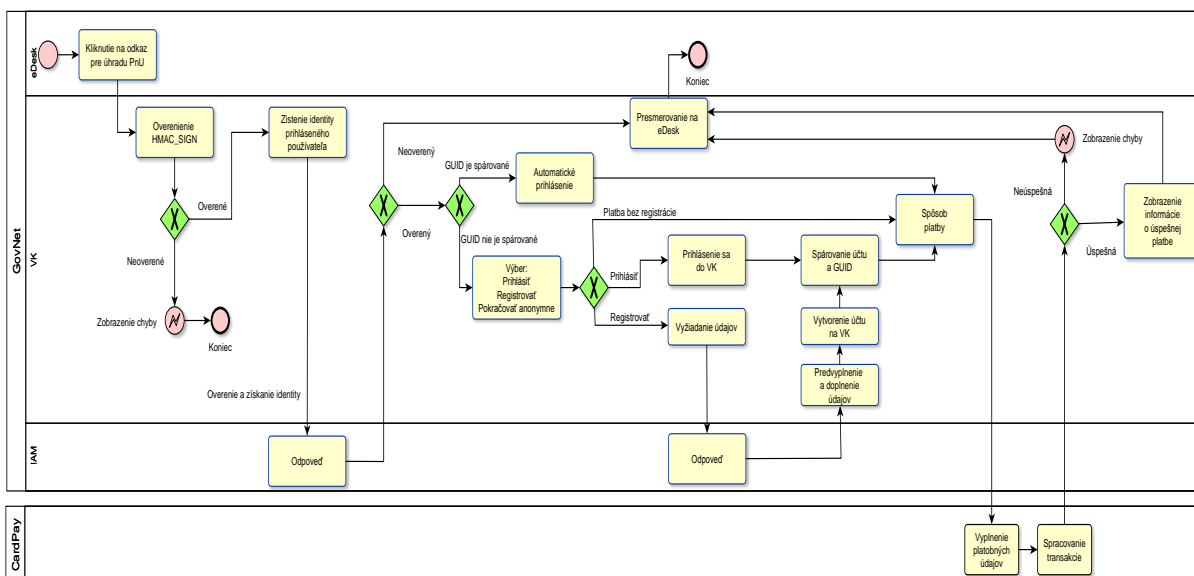
Dopracovanie funkcionalít webovej aplikácie eKolok v súvislosti s úhradou poplatku platobnou kartou na www.slovensko.sk

- Dobudovanie federácie identít fyzických osôb, fyzických osôb podnikateľov a právnických osôb.
- Dobudovanie integrácie na IAM za účelom jednotného prihlasovania.
- Úprava a rozšírenie procesov prihlasovania a registrácie.
- Integrácia s modulom eDesk.
- Úpravy existujúcich procesov pri úhrade realizovanej za elektronické služby.

Integrácia webovej aplikácie eKolok s ÚPVS

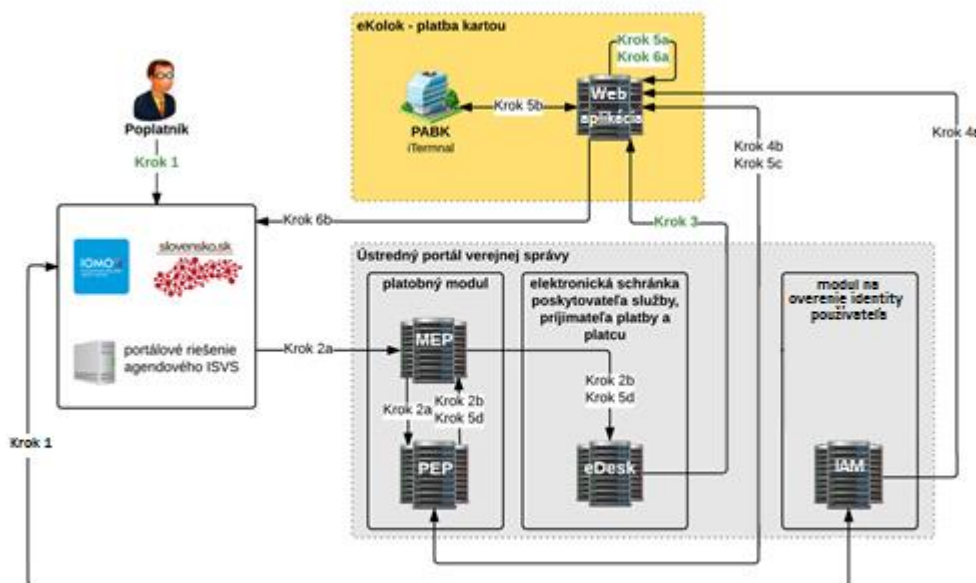
Diagram procesu PnÚ cez webovú aplikáciu eKolok

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronické služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 4/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*



Webová aplikácia eKolak integruje modul IAM za účelom automatickej identifikácie platcu pomocou SSO.

Technické riešenie a proces platby kartou sú nasledovné:



- Krok 1: Prihlásenie platcu s eID a vyžiadanie poplatnenej služby.
- Krok 2a: Vyžiadanie platobných údajov pre príkaz na úhradu (PnÚ).
- Krok 2b: Zaslanie PnÚ s platobnými údajmi do elektronickej schránky.
- Krok 3: Platca klikne na tlačítko "platba kartou" za účelom úhrady PnÚ platobnou kartou a je presmerovaný na webovú aplikáciu eKolak s platobnými inštrukciami PnÚ.

Krok 3.1 Server Slovensko.sk vo funkcii "Platba kartou" vytvorí https požiadavku na Virtuálny kiosk s parametrami VSPNU,, HMAC_SIGN.

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronicke služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 5/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*

Krok 3.2 Virtuálny kiosk overí platnosť prijatých údajov vytvorením a porovnaním HMAC_SIGN.

Krok 3.3.a Ak HMAC_SIGN nesúhlasí

Virtuálny kiosk zobrazí varovanie: „Prijatá požiadavka s chybným podpisom! Spracovanie ukončené.“ Spracovanie požiadavky sa ukončí bez návratu na RURL. RURL je nedôveryhodná, preto sa nepoužije.

Krok 3.3.b Ak HMAC_SIGN súhlasí – požiadavka je dôveryhodná

Zistí sa identita prihláseného platcu cez IAM.

- Ak sa nepodarí overenie v IAM, platca je presmerovaný späť na eDesk podľa RURL.
 - Ak sa podarí overenie, tak na základe GUID sa vyhledá platca v zozname registrovaných používateľov webovej aplikácie eKoloK.
 - Ak registrácia existuje – vykoná sa automatické prihlásenie.
 - Ak registrácia neexistuje – ponúknu sa možnosti Prihlásiť / Registrovať / Pokračovať bez registrácie.
- Krok 4a: Prihlásenie/registrácia platcu na webovej aplikácii eKoloK alebo platba bez prihlásenia podľa výberu poplatníka. Aplikácia bude integrovaná na modul IAM za účelom automatickej identifikácie používateľa pomocou SSO.

Základný scenár – platca je presmerovaný na webovú aplikáciu eKoloK, na ktorej ešte nie je registrovaný:

- a) Má možnosť zaregistrovať sa. Pri registrácii sa automaticky prepoja účty: práve vytvorený účet s identitou IAM. Po ukončení registrácie je platca presmerovaný na obrazovku úhrady.
- b) Má možnosť zvoliť si úhradu bez registrácie.

Krok 4a.A Prihlásenie alebo registrácia platcu vo webovej aplikácii eKoloK

Platcovi bude zobrazená obrazovka na prihlásenie s doplnenou možnosťou na odchod z registrácie, ale aj obídenie registrácie. Po prihlásení/registrácii bude presmerovaný na stránku úhrady.

Krok 4a.AA Manuálne prihlásiť a pridať GUID

Ak platca už má vytvorené konto vo webovej aplikácii eKoloK, môže takto spárovať konto webovej aplikácie eKoloK s identitou IAM.

Platca sa ručne prihlási do webovej aplikácie eKoloK.

Webová aplikácia eKoloK na pozadí aktualizuje používateľské konto pridaním GUID, čím sa spáruje konto webovej aplikácie eKoloK s identitou IAM pre budúce automatické prihlásenie.

Krok 4a.AB Registrovať

Platca sa ručne zaregistruje do webovej aplikácie eKoloK zadaním povinných údajov.

Webová aplikácia eKoloK automaticky predvyplní GUID a ďalšie údaje z IAM na zjednodušenie registrácie.

Alternatívny scenár 1 – platca je presmerovaný na webovú aplikáciu eKoloK, na ktorej je už registrovaný zatiaľ bez prepojenia s identitou IAM.

Platca je vyzvaný na možnosť prepojiť účty

- Po odsúhlasení budú účty automaticky prepojené.
- Webová aplikácia eKoloK informuje platcu o úspešnom prepojení účtov oznamom.
- Platca pokračuje na stránku úhrady.

Alternatívny scenár 2 – platca je presmerovaný na webovú aplikáciu eKoloK, na ktorej je už registrovaný a má previazaný účet webovej aplikácie eKoloK a identity IAM.

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronické služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 6/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*

Webová aplikácia eKoloK zistí, že platca so zaslanou identitou IAM zo Slovensko.sk už má platný účet na webovej aplikácii eKoloK s prepojením. Webová aplikácia eKoloK presmeruje platcu na stránku úhrady.

Krok 4a.B Pokračovať bez registrácie vo webovej aplikácii eKoloK

Pre správne fungovanie webovej aplikácie eKoloK sa pre GUID vytvorí konto. Ak toto konto pre GUID už existuje, použije sa. Pre jedno GUID bude existovať max. jedno konto. Pod týmto kontom sa budú zaznamenávať všetky operácie pre GUID.

Informácie budú dostupné iba pre účely prevádzky na overovanie stavu v prípade sťažností. V budúcnosti je možné po vykonaní kompletnej registrácie zobrazit' všetky doterajšie nákupy alebo ich nechať naďalej skryté, a to v závislosti od rozhodnutia objednávateľa služby.

- Krok 4b: Platca je prihlásený. Nasleduje overenie PnÚ v IS PEP (napr. či existuje a či už nie je zaplatený).
- Krok 5a: Poplatník si vyberie platbu platobnou kartou, je presmerovaný na platobnú bránu, zadá údaje z platobnej karty a zrealizuje platbu.
- Krok 5b: Potvrdenie transakcie kartovým operátorom.
- Krok 5c: Zaevidovanie úhrady PnÚ eKoloK v IS PEP a zobrazenie úspešnej úhrady PnÚ vo webovej aplikácii eKoloK.
- Krok 5d: Zaslanie informácie o úhrade PnÚ do elektronickej schránky.
- Krok 6a: Zobrazenie informácie o úspešnej úhrade PnÚ vo webovej aplikácii eKoloK a zobrazenie tlačidla „Návrat do elektronickej schránky“.
- Krok 6b: Odhlásenie poplatníka z webovej aplikácie eKoloK. Presmerovanie na návratovú adresu dodanú v kroku 3 (slovensko.sk alebo portálové riešenie IS VS) Zobrazenie informácie, že platba bola úspešná a povinná osoba automaticky spustí poskytnutie služby.

Komunikačné rozhranie

Komunikácia medzi Slovensko.sk a webovou aplikáciou eKoloK bude realizovaná:

- cez protokol HTTPS metódou POST alebo GET,
- parametre budú kódované vo forme application/x-www-form-urlencoded,
- každá požiadavka musí obsahovať autentifikačný podpis HMAC_SIGN.

Zoznam a popis parametrov požiadavky zo Slovensko.sk na webovú aplikáciu eKoloK

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
VSPNU	áno	Variabilný symbol Príkazu na úhradu	max. 10	povolené znaky: 0-9	
LANG	áno	Kód jazyka na zobrazenie aplikácie	2	prednastavená hodnota je SK. Povolené hodnoty: SK	
RURL	áno	Návratová URL			
IDGATE	áno	Pridelený identifikátor systému využívajúceho platobnú bránu (možno teraz pre potreby jednorazovej integrácie zbytočné, ale užitočné, ak by chceli danú službu využívať v budúcnosti aj pre iné systémy)			
TIMESTAMP	áno	Timestamp v UTC (časová pečiatka)	14	formát DDMMYYYYHHMISS (DDdeň, MMmesiac, YYYYrok, HHhodina, Mlminúta,SSsekunda)	
HMAC_SIGN	áno	Podpis všetkých odoslaných parametrov		algoritmus na podpis HMACSHA256	

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronicke služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 7/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*

Zoznam a popis parametrov ODPOVEDE z webovej aplikácie eKolak na Slovensko.sk

Názov	Povinný	Popis	Dĺžka	Pravidlá	Príklad
VSPNU	áno	Variabilný symbol Príkazu na úhradu	max. 10	povolené znaky: 0-9	
TIMESTAMP	áno	Timestamp v UTC (časová pečiatka)	14	formát DDMMYYYYHHMISS (DDdeň, MMmesiac, YYYYrok, HHhodina, Mlminúta,SSsekunda)	
RES	áno	Výsledok spracovania (0 – OK, iná hodnota je kód chyby)			
HMAC_SIGN	áno	Podpis všetkých odoslaných parametrov		algoritmus na podpis HMACSHA256	

Vytvorenie a overenie podpisu HMAC_SIGN

Funkčná požiadavka: Platca prihlásený na portál Slovensko.sk musí byť automaticky identifikovaný a prihlásený do webovej aplikácie eKolak podľa GUID.

Na zabezpečenie automatického prihlásenia musí byť medzi Slovensko.sk a webovou aplikáciou eKolak dôveryhodná komunikácia. Dôveryhodnosť odosielateľa bude realizovaná podpisom odosielanej požiadavky pomocou HMACSHA256 a spoločným tajným bezpečnostným kľúčom HMAC_KEY (64 bajtov). Musí byť zaručené bezpečné dodanie HMAC_KEY na oba servery Slovensko.sk a webovú aplikáciu eKolak.

Postup vytvorenia podpisu HMAC_SIGN v *Kroku 3.1*

1. Vytvoriť **reťazec na podpis** z hodnôt odosielaných atribútov VSPNU+...+IDGATE+TIMESTAMP pre požiadavku zo Slovensko.sk a VSPNU+TIMESTAMP+RES pre odpoveď z webovej aplikácie eKolak.
2. Vytvoriť podpis HMAC_SIGN, postup v Java prevzatý z http://www.tatrabanka.sk/tatrapay/TatraPay_tecnicka_prirucka_HMAC.pdf

```
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
byte[] keyBytes = hex2bytes(HMAC_KEY);
SecretKeySpec keySpec = new SecretKeySpec(keyBytes, "HmacSHA256");
Mac mac = Mac.getInstance("HmacSHA256");
mac.init(keySpec);
byte[] hmacBin = mac.doFinal(retazec_na_podpis.getBytes());
String HMAC_SIGN = bytes2hex(hmacBin); // konverzia do hexadecimál reťazca
```

Overenie prijatej požiadavky:

Na strane príjemcu sa z prijatých atribútov rovnako vytvorí **reťazec na podpis** a vygeneruje HMAC_SIGN. HMAC_SIGN sa potom porovná s prijatým HMAC_SIGN a pokračuje podľa krokov 3.2.

Príklad požiadavky:

https://ADRESA_PORTALU/URL_SLUZBY?RURL=https://www.slovensko.sk/vysledok.aspx&LANG=SK&VS=11111&PAYMENTMETHOD=CARD&ID=UPVS&SIGN=AA2BCCDD

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronické služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 8/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*

Príklad odpovede:

https://NAVRATOVA_ADRESA/URL_SLUZBY?VS=11111&RES=0&SIGN=CCDD01A3

Vyššie uvedený popis riešenia môže byť upravený/korigovaný v závislosti od dohody s treťou stranou, na informačné systémy ktorej sa integruje webová aplikácia eKolok.

Súčasťou riešenia je aj úprava popisu funkcií webovej aplikácie eKolok spôsobom, aby používanie webovej aplikácie eKolok bolo pre platcu jednoduché a zrozumiteľné. Webová aplikácia eKolok bude obsahovať nápovedy, aby platca vedel bez problémov a rýchlo vykonať úhradu platobnou kartou.

Súčasťou výstupov v súlade s predmetom Zmluvy je okrem softvéru aj príslušná dokumentácia, a to najmä:

- Detailná funkčná špecifikácia.
- Používateľská dokumentácia.
- Prevádzková dokumentácia.

Parafy:	Zmluva o dielo systém na zabezpečenie úhrady správnych a súdnych poplatkov prostredníctvom platobnej karty za elektronické služby vyžiadané cez Slovensko.sk	Odborný garant: Ú GRaF-SIT
	Strana 9/9	Číslo v CEEZ: 979/2017 Klasifikácia informácií: *V*