DEŽELNA BANKA SLOVENIJE

Uveljavitev dveh novih plačilnih storitev v okviru odprtega bančništva »Open banking« in zahteve po močni avtentikaciji
~Vprašanja in odgovori~

I. Odprto bančništvo –»Open banking«

Kaj je PSD2?

Področje plačilnih storitev se tehnološko hitro spreminja. Za povečanje konkurenčnosti, spodbujanje inovacij in večjo zaščito uporabnikov je Evropska Unija (EU) sprejela Direktivo o plačilnih storitvah 2 (Payments Service Directive 2, v nadaljevanju PSD2), skupaj z več delegiranih aktov (regulatornih tehničnih standardov, v nadaljevanju RTS). PSD2 je bila v slovenski pravni red implementirana v okviru Zakona o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (v nadaljevanju ZPlaSSIED).

Kaj prinaša PSD2?

V skladu s PSD2 mora banka za račune, ki uporabljajo spletno ali mobilno banko, omogočiti **dve novi plačilni storitvi:**

- **storitev odreditve plačil -** storitev za odreditev plačilnega naloga na zahtevo uporabnika plačilnih storitev[1] v breme plačilnega računa, odprtega pri drugemu ponudniku plačilnih storitev[2],

- **storitev zagotavljanja informacij o računih** - spletna storitev zagotavljanja informacij o plačilnih računih, ki jih ima uporabnik plačilnih storitev pri drugem ponudniku plačilnih storitev, omogoča pa vstop nebančnih institucij z namenom izvedbe plačila in zagotovitve informacije o računu.

Banke moramo pri izvajanju plačilnih storitev upoštevati tudi dodatne varnostne ukrepe glede **močne avtentikacije** uporabnikov plačilnih storitev in varnega komuniciranja, kar določajo RTS (regulatorni tehnični standardi).

Kaj prinašata novi storitvi?

Storitvi se v skladu z zakonskimi zahtevami izvajata preko tretjega ponudnika plačilnih storitev (v nadaljevanju TPP)[3], ki je lahko nebančni ponudnik ali druga banka, ki je registrirana za izvajanje dveh novih plačilnih storitev.

Uporabnik bo lahko pri TPP na enem mestu preko spletnega portala ali mobilne aplikacije upravljal enega ali več svojih računov, ki jih ima odprte v bankah in hranilnicah znotraj območja EU (vpogled v stanje in izvajanje plačil). Če ima uporabnik račune pri več bankah, bo od posamezne banke odvisen obseg podatkov, ki mu jih bo prikazala preko TPP-ja. Banke smo sicer TPP-jem dolžne posredovati tak nabor podatkov, kot jih prikazujemo v bančnih aplikacijah (npr. v spletni in mobilni banki).

Kaj je storitev zagotavljanja informacij o računih?

Pri zagotavljanju podatkov o računih se uporabniku plačilnih storitev v strnjeni in uporabniku prijazni obliki zagotovijo podatki o enem ali več plačilnih računih, ki jih ima pri enem ali več ponudnikih plačilnih storitev, ki vodijo račune. Glede na zakonske zahteve smo kot banka dolžni TPP zagotavljati naslednje informacije o računih – vse samo izrecno na predhodno privolitev uporabnika, in sicer:

- podatke o računu,
- podatke o podrobnosti računa,

[1] Uporabnik plačilnih storitev – komitent banke, ki je uporabnik spletne oz. mobilne banke in preko TPP uporablja nova tipa plačilnih storitev.
[2] Ponudnik plačilnih storitev – banka ali hranilnica
[3] Tretji ponudniki storitev – TPP (izraz "tretji" se uporablja, ker gre za tretjo osebo, ki se pojavi kot vmesni člen v informacijskem toku med imetnikom računa in ponudnikom plačilnih storitev, ki mu ta račun vodi) ponujajo dva osnovna tipa storitev, ki ju opredeljuje ZPlaSSIED (zagotavljanje podatkov o računih in storitev odrejanja plačil).

- seznam transakcij računa,
- podrobnost transakcije,
- stanje na računu,
- status plačila.

Kaj je storitev odreditve plačil?

Storitev odreditve plačil pomeni, da TPP na zahtevo plačnika odredi plačilno transakcijo, in sicer v breme plačilnega računa, ki ga ima ta plačnik odprtega pri svojem ponudniku plačilnih storitev.

Kaj mora uporabnik vedeti pri uporabi obeh novih storitev?

V primeru, da uporabnik TPP dovoli dostop do podatkov svojega računa in izvajanje transakcij, **je zaradi tega uporabnik izpostavljen različnim operativnim in varnostnim tveganjem**. Priporočamo, da se uporabnik predhodno informira:

- **kako so zaupni podatki uporabnika pri tretjem ponudniku plačilnih storitev zaščiteni** (povečano tveganje prinaša grožnjo razkrivanja osebnih bančnih podatkov tretjim osebam - med bančne podatke spadajo tudi gesla, PIN-i in drugi podatki, ki jih uporabnik uporablja za dostop do bančnih storitev),
- ali ponudnik, ki mu bo uporabnik dovolil dostop do podatkov o svojem računu, sledi najvišjim standardom varnosti z uporabo sistemov za preprečevanje tveganj,
- **ali ima ponudnik ustrezno licenco lokalnega nadzornega organa,** ki bo predvidoma na svojih spletnih straneh tudi objavil register licenciranih ponudnikov,
- **o varnostnih ukrepih**, **ki jih TPP zagotavlja v vseh fazah** dostopa do plačilnih računov uporabnika,
- z načinom preklica izmenjave in načinom reševanja sporov v primeru reklamacij ter morebitnih zlorab,
- o nadomestilih za izvršitev plačilne transakcije, ki je posledica storitve odreditve plačila preko TPP - uporabnik nosi strošek izvršitve plačilne transakcije v breme svojega transakcijskega računa pri svoji banki,
- o Urniku izvršitve plačilne transakcije, odrejene preko TPP - vsaka plačilna transakcija se bo poravnala preko obstoječih plačilnih sistemov in v skladu z urniki plačilnih sistemov. V primerjavi s poslovanjem preko spletne in mobilne banke je razlika za uporabnika samo v tem, da bo transakcijo odredil preko novega kanala (preko tretjega ponudnika plačilnih storitev), namesto preko spletne ali mobilne banke. Naprej pa bo izvršitev transakcije potekala popolnoma enako, pod enakimi pogoji in stroški.

Banka TPP ne sme neutemeljeno ovirati pri dostopanju do računov uporabnikov plačilnih storitev. TPP pa lahko pridobiva informacije o računih in v imenu uporabnika odreja plačilne transakcije le **ob uporabnikovem izrecnem soglasju**. O vsakršnih zlorabah ali neodobrenih plačilnih transakcijah nas mora uporabnik obvestiti takoj, ko je mogoče.

S čem uporabnik soglaša?

Ponudnik storitve odreditve plačil bo moral predhodno pridobiti privolitev uporabnika za dostop do podatkov o njegovem plačilnem računu. Uporabnik določa s soglasjem, do katerih podatkov o svojem plačilnem računu bo dovolil dostop tretjemu ponudniku. Ta se bo povezal prek vmesnika uporabnikove banke, ki mu bo samo omogočila dostop do zahtevanih informacij, ko bo postopek »močne« avtentikacije uporabnika uspešno zaključen. Uporabnik s potrditvijo zahteve v namenski aplikaciji svoji banki posreduje navodila, katero vrsto dostopa naj zavrne in katero sprejme. Uporabnik ima možnost, da dostop TPP-jev kadarkoli prekliče.

Pomembno je, da uporabnik pri uporabi obeh novih storitev razume, s katerimi pogoji soglaša in ne zgolj obkljuka »strinjam se«, saj lahko hitro omogoči dostop v obsegu, ki ga dejansko ne želi.

Kje najde uporabnik ponudnika z ustrezno licenco nadzornega organa?

Register ponudnikov plačilnih storitev bo javno objavljen na spletni strani Banke Slovenije.

Kako uporabnik dostopa do svoje banke?

Uporabnik bo v okviru postopka izvedbe novih plačilnih storitev preko namenske spletne aplikacije **Moj DBS** prejel in odobril ali zavrnil izvedbo plačilnih storitev, ki jih je v izvedbo posredoval preko TPP. Dostop do nove spletne aplikacije bodo imeli le uporabniki spletne in mobilne banke, ki za vstop uporabljajo prijavno sredstvo Rekono (Rekono bo nadomestil vse dosedanje načine prijave v spletno in mobilno banko) ter imajo ustrezno pooblastilo za izvajanje novih plačilnih storitev.

Kako deluje povezava med TPP in uporabnikovo banko?

Banka je v sodelovanju z zunanjim razvijalcem pripravila programsko rešitev, ki omogoča varno izmenjavo informacij za potrebe povezave med TPP in banko. Dolžnost TPP je, da za vzpostavitev povezave med lastno rešitvijo in banko uporabi namensko programsko rešitev banke, ki jo mora implementirati skladno z navodili razvijalca, da je zagotovljen varen prenos podatkov.

Uporabnik bo s TPP sklenil pogodbeno razmerje v obliki soglasja, v katerem bo določil obseg dostopa do svojih podatkov. Šele nato bo na strani banke sledilo preverjanje pristnosti stranke z uporabo močne, večfaktorske avtentikacije, ki z uporabo vsaj dveh elementov dodatno preprečuje zlorabo spletnih storitev s prestrezanjem oz. krajo varnostnih poverilnic (geslo, PIN itd.).

Banka v skladu z zakonodajo nadzoruje svoje sisteme in spremlja izvajanje plačilnih transakcij.

V okviru Združenja bank Slovenije je bil pripravljen video klip, ki je objavljen tudi na spletni strani banke na: https://www.dbs.si/produkt/novosti-psd2#tab_dodatne-informacije

Kako in v kakšnem obsegu so uporabniku prikazani podatki?

Uporabnik bo preko TPP, preko katerega bo uporabljal obe novi storitvi, pridobival podatke v enakem obsegu, kot mu jih banka prikazuje v bančni aplikaciji.

Kakšni bodo stroški za uporabnika?

Uporabnik bo nosil stroške izvrševanja transakcij v enaki višini, kot veljajo danes pri transakcijah, ki jih poravnava preko npr. elektronske ali mobilne banke.

II. Močna avtentikacija (overitev) uporabnika

Kaj je močna avtentikacija?

Močna avtentikacija uporabnika je postopek, ki temelji na uporabi dveh ali več elementov, ki spadajo v kategorijo:

- znanja uporabnika (nekaj, kar **ve samo uporabnik**, npr. statično geslo, koda, osebna identifikacijska številka);
- lastništva uporabnika (nekaj, kar je v **izključni lasti uporabnika**, npr. pametna kartica, mobilni telefon);
- neločljive povezanosti z uporabnikom (nekaj, kar **uporabnik je**, npr. biometrična značilnost, kot je prstni odtis).

Zakonsko predpisana uporaba močne avtentikacije na področju celotnega evropskega gospodarskega prostora prispeva k zmanjšanju zlorab pri izvajanju plačilnih storitev na daljavo.

V okviru postopka avtentikacije uporabnika pri izvajanju storitev, odrejenih preko naslednjih kanalov: TPP, DBS NET, DBS PRONET in mDBS bo banka v primeru petih zaporednih napačnih prijav onemogočila izvajanje storitev preko izbranega kanala tako za vstop v izbrani kanal kot potrjevanje transakcij. Za ponovno vzpostavitev uporabe posameznega kanala se uporabnik oglasi osebno v poslovalnici banke.

Kako uporabnik vstopa v DBS NET, DBS PRONET in mDBS?

Pri vstopu v spletno in mobilno banko se izvaja močna avtentikacija uporabnika, v okviru katere se uporabnik predstavi z naslednjima dvema elementoma:

- nekaj, kar **ve samo uporabnik,**
- nekaj, kar je v **izključni lasti uporabnika.**

Kako uporabnik potrjuje plačilne transakcije v DBS NET, DBS PRONET in mDBS?

Uporabnik Rekono spletne osebne izkaznice bo preko spletne ali mobilne banke za vsako novo plačilo izvedel dodatno varnostno potrditev, ki jo uporabnik prejme v obliki SMS-varnostne kode. Za vse transakcije, ki so shranjene v uporabnikovem imeniku plačil, pa dodatno potrjevanje ne bo potrebno.

Kako uporabnik potrjuje zahtevek za izvajanje plačilne transakcije, odrejene preko TPP?

Za plačila, odrejena preko TPP, bo potrebna še dodatna potrditev z enkratnim geslom. Uporabnik bo ob izboru načina plačila s strani TPP preusmerjen na svojo banko, kjer se bo avtenticiral (na enak način, kot pri dostopu do bančnih rešitev), potrdil izvedbo zahteve za izbrani TPP ter pregledal in z enkratnim geslom potrdil zahtevek za izvedbo plačilne transakcije. Uporabnik ima v tem procesu možnost preklicati izvedbo zahteve za plačilo.

V primeru, ko uporabnik opravi plačilno transakcijo preko TPP kanala in se kasneje, kljub že potrjenemu nalogu za plačilo, odloči za preklic transakcije, lahko preklic izvede preko TPP. V kolikor je preklic plačila še možno opraviti, bo banka po prejemu zahtevka za preklic izvedbo plačila preklicala.

Ljubljana, 25. 11. 2019