BKS Bank

BKS Bank AG,
Glavna podružnica Hrvatska
Mljekarski trg 3, HR-51000 Rijeka
Sjedište osnivača: St. Veiter Ring 43
A-9020 Klagenfurt, Austrija

Tel.: ++385 51 353 555
Fax: ++385 51 353 566
info@bks.hr
www.bks.hr

IBAN: HR57 2488 0011 0111 1111 6
SWIFT: BFKKHR22
OIB: 02138784111
VAT ID: HR 02138784111
MBS: 040364313 pri Trgovačkom sudu u Rijeci

BKS Bank – sigurni s nama

Rijeka, srpanj 2019.

1. Sadržaj

2. BKS online

BKS online je skup usluga koje korisniku omogućavaju korištenje usluga Banke putem interneta. BKS BizzNet namijenjen je pravnim osobama koje su klijenti BKS Bank AG, Glavna podružnica Hrvatska (koji u BKS Banci imaju otvoren transakcijski račun). BKS MyNet namijenjen je fizičkim osobama koje su klijenti BKS Bank AG, Glavna podružnica Hrvatska (koji u BKS Banci imaju otvoren račun za plaćanje).
Za pristupanje uslugama BKS BizzNet za pravne osobe potrebno je:

- Ispuniti BKS BizzNet pristupnicu
- Zahtjev za izdavanje certifikata – ispuniti u 2 primjerka
- Ugovor o obavljanju usluga certificiranja – ispuniti u 2 primjerka
- Preslika dokumenta (osobna iskaznica, vozačka dozvola ili putovnica) na kojoj je vidljiv Vaš JMBG ili OIB

Za pristupanje uslugama BKS MyNet za građanstvo potrebno je:

- ispuniti BKS MyNet Pristupnicu

Pristupnicu, obrasce i upute za njihovo ispunjavanje moguće je preuzeti preko naše internet stranice www.bks.hr ili u poslovnicama Banke.

Mogućnosti BizzNet usluge:

- pregled stanja po transakcijskim računima;
- pregled prometa po transakcijskim računima;
- pregled i ispis izvoda po transakcijskim računima;
- plaćanje računa u domaćem platnom prometu;
- plaćanje kunskih/deviznih računa;
- plaćanje pojedinačnim unosom
- slanje zbrojnog naloga u SEPA (PAIN.001) formatu;
- preuzimanje izvadaka u SEPA (CAMT.053) formatu;
- pregled i kontrola svih naloga za plaćanje;
- istovremeno potpisivanje većeg broja naloga;
- pregled aktualne tečajne liste BKS Bank AG, Glavna podružnica Hrvatska i Hrvatske narodne banke;
- zadavanje naloga za plaćanje unaprijed, uz mogućnost opoziva prije datuma izvršenja;
- trenutno provođenje plaćanja na račune drugih sudionika platnog prometa koji imaju otvoren račun kod BKS Bank AG, podružnica Hrvatska

Prednosti internet bankarstva:

- dostupnost 24 sata dnevno;
- mogućnost slanja naloga koji će se izvršiti na određeni datum;
- mogućnost ugovaranja različitih ovlaštenja za zaposlenike od strane klijenta (ovlaštenje za unos naloga, ovlaštenje za potpisivanje naloga, ovlaštenje za uvid u stanje i promet po računu, ovlaštenje za pregled i povlačenje izvoda);
- sve naknade su povoljnije u odnosu na standardne tarife naknada za naloge preko šaltera;
- ušteda vremena i putnih troškova;
- jednostavniji, brži i ekonomičniji način poslovanja

3. Sigurnost

Korisniku je jako važna sigurnost, pogotovo kad se o financijama, pa je jasan i strah i nepovjerenje korisnika u internet bankarstvo, osobito kada se zna da je najrašireniji oblik „cyber“ zločina upravo krađa identiteta.
Na povećanju stupnja sigurnosti i ograničavanju napada na zatvorene sustave se već dugo radi na globalnoj razini, no banke posebno budno paze na zaštitu kako svojih podataka, tako i podataka korisnika.
Povjerljivi se sadržaji općenito nastoje zaštititi od neautoriziranih osoba na način da se šifriraju. Pošiljatelj šifrira sadržaj poruke prije njena slanja, a primatelj je dešifrira po primitku. Eventualne treće osobe na mreži mogu vidjeti samo šifrirane podatke.
Osim zaštite tajnosti sadržaja, sustavi za šifriranje poruka upotrebljavaju se i radi utvrđivanja identiteta sugovornika te radi sprječavanja neovlaštene izmjene sadržaja. U procesu komunikacije važno je biti siguran da je udaljeni primatelj/pošiljatelj stvarno onaj za kojeg se predstavlja, a ne netko tko je presreo poruku te je može izmijeniti ili može pročitati brojeve kreditnih kartica koje kasnije može zloupotrijebiti. U ovu se svrhu upotrebljava **elektronički potpis**.
Elektronički potpis je skup podataka u elektroničkom obliku. Ti su podaci pridruženi ili logički povezani i služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta. Realizirani su preko PKI (Public Key Infrastructure) tehnologije na kojoj se temelje **smart-kartice/USB Smart Card čitač** i **tokeni** (sigurnosne kartice).
PKI tehnologija temelji se na smart-karticama/smart-čitačima [Smart Card] s certifikatima, koje svaki korisnik usluge dobiva u procesu certifikacije. Za korištenje pametne kartice potreban je PIN [Personal Identification Number] kojeg posjeduje samo korisnik - vlasnik smart-kartice/smart-čitača. Zaštita i čuvanje smart-kartice/smart-čitača i PIN-a obveza su svakog korisnika usluge. Primjenom smart kartica/smart čitača privatni ključ nikada ne „napušta“ karticu/čitač i digitalni se potpis generira na čip unutar zaštićenog područja.
Korisnici elektroničkog bankarstva u svojstvu fizičkih osoba koriste uslugu upotrebom skupa sigurnosnih uređaja koji čine: token, korisničko ime i lozinka.
Token je autentifikacijsko/ autorizacijski uređaj neophodan za pristup uslugama elektroničkog bankarstva i autorizaciju naloga. Korištenjem tokena kreira se jednokratni sigurnosni kod potreban za prijavu u aplikaciju. Pored sigurnosnog koda Banka korisniku dodjeljuje i korisničko ime kao identifikacijski broj. Lozinka je tajni identifikacijski podatak koji je poznat isključivo Korisniku.
Pitanja koje se pri korištenju Internet bankarstva nameću su sljedeća: Kako biti siguran pripada li javni ključ zaista korisniku, odnosno nije li zloupotrebljen od strane druge osobe? Je li korisnik siguran da doista komunicira sa svojom bankom? Zbog toga korisnici imaju **certifikate** koji služe za identifikaciju. Certifikati ih povezuju s njihovim javnim ključem. Sam proces certifikacije korisnika odvija se osobno i podrazumijeva pouzdano identificiranje korisnika prije nego što mu se izda pametna kartica s certifikatom. Pomoću pametne kartice i instaliranog čitača pametnih kartica, korisnik se prijavljuje u BKS BizzNet aplikaciju, a pomoću tokena (hardverskog ili softverskog) potpisuje svaki dokument [financijski ili nefinancijski nalog] koji se razmjenjuje s BKS Bank AG, Glavna podružnica Hrvatska.

U Web-sustavima algoritmi se koriste u konkretnim proizvodima za zaštitu podataka tijekom prolaska Internetom. Jedan od njih je Secure Socket Layer (SSL) kojeg koristi i naša Banka. Razvijen je i sustav Transport Layer Security (TLS) pomoću kojeg se nastoje riješiti problemi vezani uz sigurnost. Protokol HTTP nadovezuje se na sigurnosni sloj TLS i obično se naziva HTTPS ili Secure HTTP.

Svaki nalog koji se kreira prije izvršavanja elektronički potpisuje jedan ili više korisnika. Time se osigurava neporecivost, odnosno onemogućava pobijanje činjenice o kreiranju i slanju naloga.

4. Automatska odjava

Ukoliko nakon prijave više od 5 za MyNet odnosno 15 minuta za BizzNet ne koristite aplikaciju (primjerice nešto hitno morate obaviti na nekom drugom mjestu), sigurnosni protokol automatski će Vas odjaviti. Kako bi nastavili rad, morat ćete ponoviti prijavu. Na taj će se način spriječiti neželjeni uvid u preglede po Vašim računima i transakcijama za vrijeme kada Vi niste prisutni za računalom.

5. Zaštita podataka

Korištenjem tehnologije elektroničkog potpisa osigurana je neizmjenjivost svih podataka koje korisnici usluge BKS online servisa razmjenjuju preko Interneta. Da bi se podaci koji se razmjenjuju zaštitili i od neovlaštenog čitanja, za njihov prijenos koristi se SSL protokol. Uporabom navedenog protokola svi podaci koje korisnik izmjenjuje s Bankom u svakom su trenutku enkriptirani. Enkripcija podataka obavlja se pomoću tajnog ključa koji na slučajan način kreira korisnikov pretraživač i to prigodom svakoga spajanja na poslužitelj. Tajni ključ dostavlja se poslužitelju zaštićen tehnikom enkripcije javnim i privatnim ključevima. Za uspješno uspostavljanje SSL veze s provjerom autentičnosti poslužitelja korisnik mora koristiti pretraživač novijeg datuma. Korisnik može provjeriti odgovara li njegov pretraživač zahtjevima tako da unutar naslovne web stranice klikne mišem na sličicu za provjeru pretraživača. Indikator uspješno uspostavljene SSL veze prikazuje se kao sličica zatvorenog lokota u krajnjem donjem dijelu korisnikova pretraživača.

6. Podrška

BKS Bank AG, Glavna podružnica Hrvatska svojim korisnicima osigurava servis za rješavanje svih nejasnoća i problema te pružanje informacija korisnicima pod nazivom Podrška.
Isključivi cilj tima Podrške je održavanje zadovoljstva klijenata, korisnika usluge Internet bankarstva, na veoma visokoj razini. Na usluzi smo Vam svaki dan u radnom vremenu od 08.00 do 16.00 sati. Telefonski broj Podrške je 0800/ 257 257, za pozive iz inozemstva +385 51/353 555.

Što korisnik može učiniti?

Sve prethodno navedeno mjere su koje Banka poduzima da bi klijentima osigurala dovoljnu razinu zaštite i sigurnosti. Slijedi popis radnji koje i sam korisnik može i koje je potrebno učiniti da bi zaštitio svoje podatke, a time i sebe:

- čuvajte svoju Smart karticu (Smart čitač) / token i odlažite je nakon upotrebe na sigurno mjesto;
- čuvajte svoju lozinku;
- lozinku pažljivo sastavite - nije poželjno koristit svoje osobne podatke, kao što su broj telefona, ime ili adresa., preporučuje se da lozinka bude kombinacija različitih brojeva s najmanje 6 znamenki;
- zapamtite Vaše korisničke podatke - ne zapisujte ih, ne dijelite ih s drugima i nemojte ih pohranjivati na računalu;
- redovno instalirajte sigurnosne zakrpe za operacijske sustave i aplikacije;
- koristite kvalitetne antivirusne programe i redovito ih dopunjujte novim definicijama virusa;
- ne šaljite tajne podatke, kao što su lozinke ili brojevi kartica, e-mailom poštom ili koristeći socijalne mreže (npr. Facebook,Twitter, Linkedin...) jer ih je moguće presresti i zloupotrijebiti;
- ne koristite Vaše korisničke podatke za pristup drugim online programima ili stranicama;
- izbjegavajte preuzimanje programa s Interneta iz nepoznatih izvora;
- kada ste završili s korištenjem računala, ne ostavljajte ga u stanju mirovanja već ga isključite;
- ukoliko sumnjate da je neovlaštena osobe došla u posjed Vaše lozinke, možete je promijeniti unutar aplikacije za Smart karticu/ Smart čitač ili blokirati pristup sustavu;

- ukoliko smatrate da je neovlaštena osoba došla u posjed Vaše lozinke ili tokena, možete promijeniti lozinku unutar aplikacije elektroničkog bankarstva ili blokirati pristup sustavu unošenjem izmišljene lozinke/ sigurnosnog koda 4 puta uzastopce;
- blokadu također možete zatražiti u poslovnicama Banke ili pozivom na 0800 257 257, za pozive iz inozemstva +385 51 353 555 u radno vrijeme Banke;
- u slučaju bilo kakve nedoumice ili sumnje u zloupotrebu MyNet ili BizzNet usluge obavezno kontaktirajte Banku

7. Ključni pojmovi

PIN – osobni identifikacijski broj koji se koristi za aktivaciju smart kartice. Ne preporuča se dijeljenje informacije o PIN-u s drugima. U slučaju da ga zaboravite možete tražiti novi, ili možete promijeniti postojeći, ako smatrate da postoji opasnost da ga netko drugi zna i da ga može zloupotrijebiti.
SMART („pametna“) kartica/čitač – kartica/čitač koja/koji ima ugrađen čip s dva snimljena ključa – tajni i javni. Tajni sadrži opće podatke o korisniku, a privatnim korisnik potpisuje svaku izvedenu transakciju.
Identifikacija – sam proces unosa imena korisnika i jednokratne lozinke koju ispisuje token uređaj ili pametna kartica/pametni čitač.
Autentifikacija – postupak u kojem se ispituje je li korisnik koji pristupa e-računima doista vlasnik tih računa.
Elektronički potpis – u internet bankarstvu ima jednaku vrijednost kao vlastoručni potpis u stvarnom svijetu. Sastoji se od niza podataka koji potvrđuju identitet, autentičnost i neporecivost slanja i primanja određenog dokumenta tijekom e-poslovanja.
Korisničko ime je identifikacijski broj Korisnika koji dodjeljuje Banka.
Lozinka je tajni identifikacijski podatak koji je poznat isključivo Korisniku.
Token je autentifikacijsko/ autorizacijski uređaj neophodan za pristup uslugama elektroničkog bankarstva i autorizaciju naloga, u vlasništvu je Banke i Korisnik ga je dužan vratiti na zahtjev Banke.

Čitač kartica i primjer **SMART kartice**

Primjer tokena

USB **SmartCard čitači**