TEHNIČNE ZAHTEVE ZA SISTEME SPLETNEGA IN MOBILNEGA BANČNIŠTVA

Avgust, 2024

UniCredit Banka Slovenija d.d.

Ameriška ulica 2
SI-1000 Ljubljana
Slovenija

Tel.: +386 1 5876 600 Faks: +386 1 5876 684 Registrirana pri Okrožnem sodišču v Ljubljani št.reg.vl. 1/10521/00, Osnovni kapital družbe 20.383.764,81 EUR, Matična številka 5446546000, ID številka za DDV SI59622806.

UniCredit Bank

UVOD

Za nemoteno delovanje sistemov spletnega in mobilnega bančništva je potrebno zadostiti minimalnim zahtevam glede potrebne strojne in programske opreme. V nadaljevanju so te zahteve opisane za vsak sistem posebej in veljajo le za opisani sistem.

1. TEHNIČNE ZAHTEVE ZA PROGRAM E-BANK PERSONAL/CORPORATE

1.1. Enouporabniška rešitev - E-bank/Personal

- osebni računalnik z nameščenim operacijskim sistemom Windows 8.1, Windows 10, Windows 11. Vsi operacijski sistemi Windows morajo biti posodobljeni na najnovejše popravke,
- programsko opremo Hal E-Bank,
- kvalificirano digitalno potrdilo na varnem mediju, izdano s strani Halcom CA,
- povezavo z bančnim strežnikom (dostop do interneta ali klicno povezavo) in
- sklenjeni poslovni dogovor o poslovanju preko Hal E-Bank rešitev, ki ga sklenete z banko.

Če vam je bilo kvalificirano digitalno potrdilo izdano na pametni kartici, potrebujete tudi čitalnik pametnih kartic (priključite ga na osebni računalnik).

ZAHTEVANA STROJNA OPREMA:

KOMPONENTA	ZAHTEVA
Računalnik in procesor	minimalno: 1 GHz priporočljivo: vsaj 2 GHz 32-bitni procesor
Pomnilnik (RAM)	minimalno: 1 GB priporočljivo: vsaj 2 GB
Trdi disk	minimalno: 1 GB priporočljivo: vsaj 2 GB nezasedenega prostora
Zaslon	minimalno: 1024 x 768 pik
Dodatne zahteve	Internetna povezava. V primeru modemske povezave z internetom je potrebno, da modem podpira hitrost prenosa minimalno 128 Kbps, priporočljivo 512 Kbps.
	Če vam je bilo kvalificirano digitalno potrdilo izdano na pametni kartici, potrebujete tudi čitalnik pametnih kartic (priključite ga na osebni

ZAHTEVANA PROGRAMSKA OPREMA:

Za namestitev programske opreme so potrebne ustrezne pravice za nameščanje ali pa je potrebna prisotnost sistemskega administratorja.

- Nameščena mora biti programska oprema za branje pametnih kartic Nexus Personal Windows /8.1/10),
- Nameščen spletni brskalnik Microsoft Internet Explorer verzije 11.0 ali novejši,
- Nameščen Adobe Acrobat Reader ali Adobe Acrobat X verzije 10.0 ali novejši,

ZAHTEVANA POSTAVITEV PARAMETROV:

- nastavitev časovnega pasu na osebnih računalnikih s Hal E-Bank odjemalcem ali z baznim strežnikom (»Time Zone«) na GMT+1,
- nameščena (in ne nujno privzeta/»default«) podpora slovenskim področnim nastavitvam (»Regional Settings – Slovenian«) na delovnih postajah.

Pri povezavi z bančnim strežnikom preko požarnega zidu je potrebno za povezovanje odpreti zahtevana vrata za prenos podatkov in osveževanje programa. IP naslovi in številke zahtevanih vrat so navedeni v programu, ki se nahaja na naslednji povezavi:
https://www.halcom.si/si/pomoc/?action=showEntry&data=203

- Aplikacija za povezovanje ne uporablja HTTP proxy strežnikov, saj tudi osnovni protokol za prenos podatkov ni protokol HTTP.

Aplikacija se sicer lahko povezuje neposredno na HTTPS strežnik, vendar ne preko proxy strežnika. Do sedaj prejeli zelo malo zahtev po implementaciji SSL tunnelinga oziroma podpore SSL proxyjem. Z varnostnega stališča je vseeno, ali podjetje dovoli dostop do nekega URL naslova preko SSL proxy-ja ali dovoli odpiranje zunanjih povezav do točno določenega strežnika in TCP porta.

Edini proxy strežniki, ki jih odjemalec zato podpira, so t.i. "port forwarding" ali "traffic redirection" proxy strežniki, kjer se ves promet, poslan na TCP vrata proxy strežnika, v nespremenjeni obliki pošilja naprej do ciljnega ebančnega strežnika.

1.2. Večuporabniška rešitev – E-bank/Corporate

Hal E-Bank/Corporate program je namenjen za uporabo pri pravnih osebah, ki opravljajo plačilni promet na večih računalnikih lokalnega omrežja.

Hal E-Bank/Corporate program deluje v načinu odjemalec / strežnik, ki zahteva skupno bazo podatkov, običajno nameščeno na strežniku. Nanj je potrebno namestiti programsko opremo strežnika podatkovne zbirke IBM DB2 Universal Database Express Edition, na delovne postaje - odjemalce pa IBM DB2 klienta ter programsko opremo Hal E-Bank. Vso programsko opremo ter medsebojne povezave je potrebno ustrezno konfigurirati. Za namestitev so potrebne administratorske pravice na strežniku.

Dodatne zahteve za uporabo večuporabniške rešitve glede na enouporabniško rešitev. Pri tem je potrebno upoštevati vse zahteve, ki veljajo za enouporabniško rešitev!

Več informacij o tehničnih zahtevah ter namestitvi je na voljo na Halcomovi spletni strani.

ODJEMALSKI RAČUNALNIKI/DELOVNA MESTA:

Zahteve za odjemalski računalnik:

- priključeni na lokalno omrežje po TCP/IP protokolu,
- dodatno vsaj 2 GB prostora na trdem disku,
- če se za povezavo z Hal E-Bank strežnikom uporablja klicni dostop, mora na vsaj enem računalniku z nameščenim Hal E-Bank odjemalcem biti nameščen modem. V primeru da se uporablja klicni

dostop je možna izmenjava podatkov z banko samo na računalnikih na katerih so nameščeni modemi. V primeru da je modem nameščen samo na enem računalniku, poteka vsa izmenjava podatkov z banko poteka preko tega računalnika.

BAZNI STREŽNIK ZA SKUPNO BAZO PODATKOV:

Zahteve operacijskega sistema se razlikujejo glede na verzijo baze podatkov: - IBM DB2 ver. 11.1

- Windows 7 SP1 (Enterprise, Professional, Ultimate),
- Windows 8.1 (Enterprise, Professional, Standard),
- Windows 10 (Enterprise, Professional),
- Windows Server 2012 (Datacenter, Essentials, Standard),
- Windows Server 2012 R2 (Datacenter, Essentials, Standard),
- Windows Server 2016 (Datacenter, Essentials, Standard).

Zahteve za operacijski sistem za delovne postaje so enake kot za strežnik.

- Podporo TCP/IP protokolu.
- Potreben prostor na disku za namestitev programa IBM DB2 je vsaj 2 GB. Pri zahtevanem prostoru na disku za bazo podatkov je težko oceniti velikost baze zaradi možnosti sprejema datotek. Približen izračun: 5000 transakcij = 20 Mb prostora + datoteke.
- Velikost hitrega pomnilnika (RAM):
  - Windows 7 SP1/ Windows 8.1 / Windows 10 vsaj 1 GB ter za vsakega sočasnega uporabnika mrežne različice Hal E-Bank dodatne 4 MB pomnilnika RAM (priporočljivo 1,5 GB pomnilnika RAM)
  - Windows Server 2012 / 2016 vsaj 1,5 GB ter za vsakega sočasnega uporabnika mrežne različice Hal E-Bank dodatne 4 MB pomnilnika RAM (priporočljivo 2 GB pomnilnika RAM)

Priporočljiva velikost pomnilnika je odvisna tudi od ostalih aplikacij, ki se izvajajo na strežniku. Glavni pogoj je, da ima strežnik na razpolago toliko hitrega pomnilnika, da ne uporablja diska kot pomnilnika (Swap).

- Podpora slovenskim sistemskim področnim nastavitvam mora biti privzeta vsaj za čas namestitvenega postopka. (»Regional Settings – Slovenian«; »Set as system default local«)
- Baza podatkov IBM DB2.

Zaradi lažje izvedbe inštalacije je na strežniku potrebno pred prihodom tehnika:

- Kreirati mapo z imenom »EbankFiles«.
- Za vse bodoče uporabnike večuporabniške verzije Hal E-Bank/Corporate potrebno nastaviti dostop do te mape (varnost, skupna raba - uporabniki morajo imeti pravice za spreminjanje mape, podmap in datotek).
- Klient dostopa do strežnika skozi TCP/IP vrata 50000, kar pomeni, da morajo biti navedena vrata odprta na morebitnem požarnem zidu in morebitnem usmerjevalniku (router-ju), ki se nahaja med klientom in strežnikom, kjer se nahaja podatkovna baza.

1.3. Zahtevani varnostni mehanizmi pri uporabi aplikacije E-bank

Za varno uporabo aplikacije E-bank mora uporabnik:

- uporabljati protivirusno programsko opremo, ki naj se redno posodablja, v skladu z navodili proizvajalca,
- uporabljati požarni zid (izjemi sta porta 3600 in 3604, ki morata biti odprta za nemoteno delovanje)
- skladno z navodili proizvajalcev programske opreme obvezno redno posodabljate programsko opremo z rednimi in zadnjimi varnostnimi popravki,
- skrbno varovati podatke in elemente avtetikacije za vstop v program E-bank (PIN kodo, certifikat),
- geslo za dostop do aplikacije E-bank redno menjati.

Za varno uporabo varnostnega elementa (pametna kartica/USB ključ na katerem je kvalificirano digitalno potrdilo) mora uporabnik:

- kartico ali USB ključ uporabljati v čitalcu/računalniku samo takrat, ko uporablja aplikacijo E-bank,
- pred uporabo vedno preveriti, da gre za pristen program oz. spletno stran,
- po končani uporabi je potrebo program ali brskalnik takoj zapreti in obvezno odstraniti kartico ali USB ključ iz računalnika,
- kartico/USB ključ in PIN kodo hraniti ločeno (nikoli skupaj),
- PIN kodo kartice/USB ključa redno menjati.

2. TEHNIČNE ZAHTEVE ZA UPORABO ONLINE BANKE

Za brezhibno delovanje Online banke je potrebna naslednja oprema:

-
- uporabniško ime,
- žeton za generiranje gesel in PIN številko,
- dostop do interneta.

2.1.Zahtevana strojna oprema

- Internetna povezava

Internetna povezava

2.2. Zahtevana programska oprema

- Windows 7 ali novejši operacijski sistem, MacOS 10.9 ali novejši

Brskalnik	**Minimalna različica**
Chrome	51
Firefox	68
IE	11
Edge	13
Safari	7
Opera	24

- Nameščen Adobe Reader verzije 17.00 ali novejši

2.3. Zahtevane nastavitve programske opreme

- Omogočen TLSv1.2. (Transport Layer Security)protokol;

- Omogočen JavaScript;
- Omogočen prikaz pojavnih oken za spletno stran www.unicreditbank.si in https://si.unicreditbanking.net

2.4. Zahtevani varnostni mehanizmi pri uporabi aplikacije Online banka

Za varno uporabo aplikacije Online banka mora uporabnik:

- uporabljati redno posodobljeno protivirusno programsko opremo,
- uporabljati požarni zid sistema MS Windows,
-
- posodabljati vso programsko opremo z izdanimi varnostnimi popravki,
- skrbno varovati podatke in opremo za vstop v Online banko (žeton, PIN kodo, uporabniško ime).

2.5. Varnostna priporočila pri uporabi aplikacije Online banka

- V nastavitvah Online banke aktivirajte varnostno vprašanje in odgovor, ki ga poznate le vi. Svetujemo vam, da varnostna vprašanja redno preverjate in spreminjate.
- Do Online banke dostopajte izključno preko uradne spletne strani ali preko varne povezave https://si.unicreditbanking.net.
- Tretjim osebam NIKOLI ne dovolite oddaljenega dostopa do vašega računalnika.
- Spremljajte varnostna obvestila banke o morebitnih ponarejenih spletnih straneh.
- Redno skrbite za varnostne posodobitve na operacijskem sistemu in brskalniku, ki ju uporabljate za uporabo Online banke.
- Banka nikoli ne preverja vaših podatkov (številke plačilnih kartic, geslo za Online banko), po spletni pošti ali preko telefona, zato jih ne zaupajte nikomur, tudi če ste za to zaprošeni.
- Uporabite možnost, da lahko sami omejite uporabo sredstev s spremembo transakcijskega in dnevnega limita v Online banki.
- Uporabe možnost dodatnih obveščanj v Online banki. Obveščanje lahko aktivirate sami in se izvajajo preko elektronske pošte.
- V primeru kakršnih koli nepravilnostih banko nemudoma obvestite na online[at]unicreditgroup.si.
- Za več podrobnosti o informacijski varnosti vam predlagamo vam obisk in pregled vsebin na internetni strani www.varninainternetu.si in https://pazi.se/.

3. TEHNIČNE ZAHTEVE ZA UPORABO APLIKACIJ MOBILNA BANKA GO! IN MOBILNA BANKA PRO!

Za brezhibno delovanje aplikacije je potrebna naslednja oprema:

- Internetna povezava;
- Minimalno verzijo Android 5.0 Lollipop - za uporabnike pametnih naprav z operacijskim sistemom Android;
- Minimalno verzijo iOS 12 – za uporabnike pametnih naprav Apple;
- HarmonyOS 2.0 – za uporabnike Huawei pametnih naprav;

3.1. Varnostni mehanizmi pri uporabi aplikacije Mobilna banka GO! In Mobilna banka PRO!

Za varno uporabo aplikacije Mobilna banka GO! In Mobilna banka PRO! priporočamo:

- uporabo protivirusno programsko opreme za mobilne naprave,
- da mobilna naprava nima odstranjenih proizvajalčevih omejitev za dostop do delov mobilnega sistema, ki so zaščiteni (t.i. rootanje ali jailbreaking)
- da imate dostop do mobilne naprave zavarovan s varnostnim elementom (PIN koda, prstni odtis,...)
- da nameščate aplikacije samo iz uradnih trgovin z aplikacijami (nikoli preko spletnih povezav v elektronskih sporočilih)
- da redno posodabljate svoje mobilne naprave z zadnjimi posodobitvami, ki vam jih proizvajalec mobilne naprave
- da namesto odprtih dostopnih točk, raje uporabljajte podatkovno povezavo (3G, 4G, 5G) ali pa se odločite za storitev navideznega zasebnega omrežja (VPN)

3.2. Varnostna priporočila pri uporabi aplikacije Mobilna banka GO! In Mobilna banka PRO

- Uporabniških imen in PIN gesel nikoli ne shranjujte v svojo mobilno napravo
- Banka nikoli ne preverja vaših podatkov (številke plačilnih kartic, geslo za Online banko), po spletni pošti ali preko telefonskega klica, zato jih ne zaupajte nikomur, tudi če ste na tak način za to zaprošeni.
- Tretjim osebam NIKOLI ne dovolite oddaljenega dostopa do vaše mobilne naprave, tudi če je to eksplicitno zahtevano.
- Aktivirajte si varnostno vprašanje in odgovor, ki ga poznate le vi. Svetujemo vam, da varnostna vprašanja redno preverjate in spreminjate.
- Spremljajte varnostna obvestila banke o morebitnih ponarejenih spletnih straneh.
- Uporabite možnost, da lahko sami omejite uporabo sredstev s spremembo transakcijskega in dnevnega limita v Mobilni banki.
- V primeru kakršnih koli nepravilnostih banko nemudoma obvestite na online@unicreditgroup.si.
- Za več podrobnosti o informacijski varnosti vam predlagamo vam obisk in pregled vsebin na internetni strani www.varninainternetu.si in https://pazi.se/.

4. PODPORA UPORABNIKOM

Dodatna vprašanja lahko pošljete na elektronske naslove:

- e-bank@unicreditgroup.si
- online@unicreditgroup.si

ali pokličete službo za pomoč uporabnikom sistemov spletnega in mobilnega bančništva na telefon +386 1 5876 600.