CARNET

KeePass

NCERT-PUBDOC-2018-5-360

CERT.hr

Sadržaj

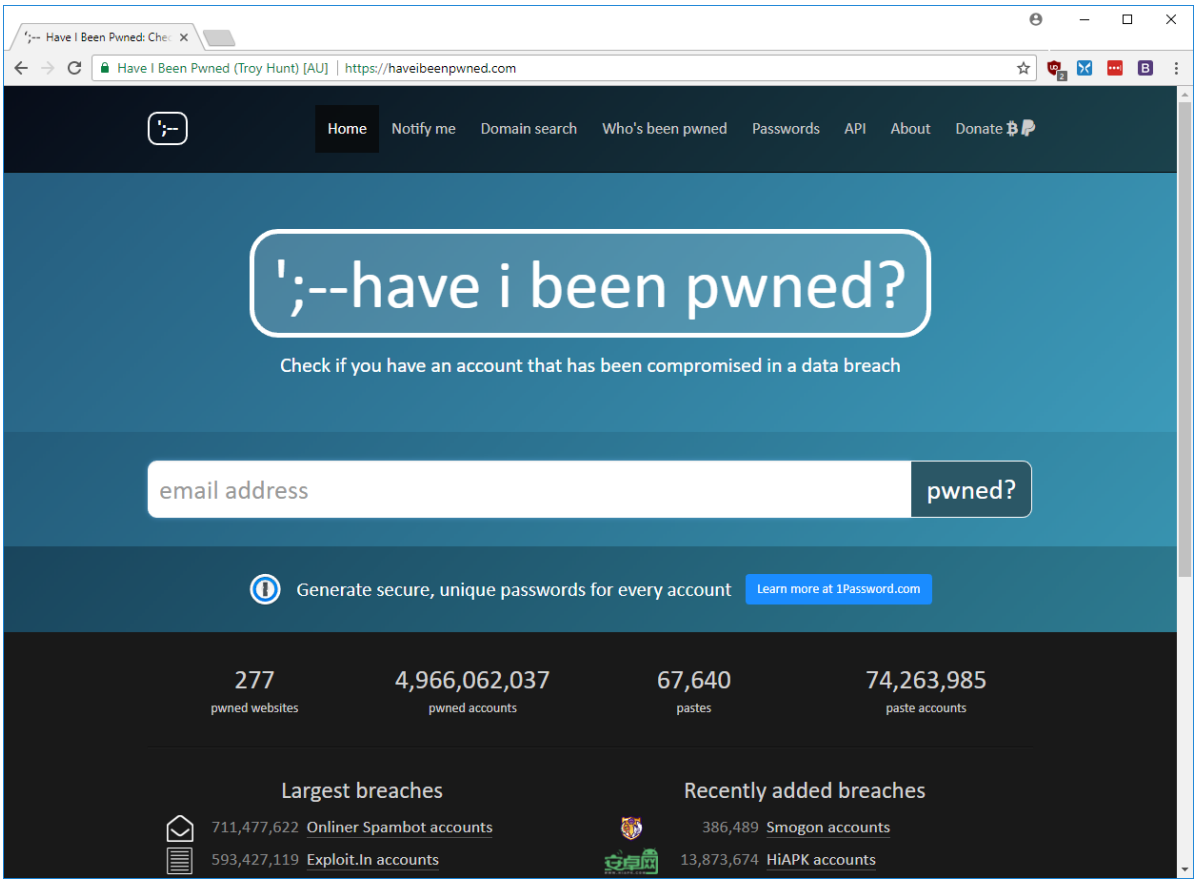
Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

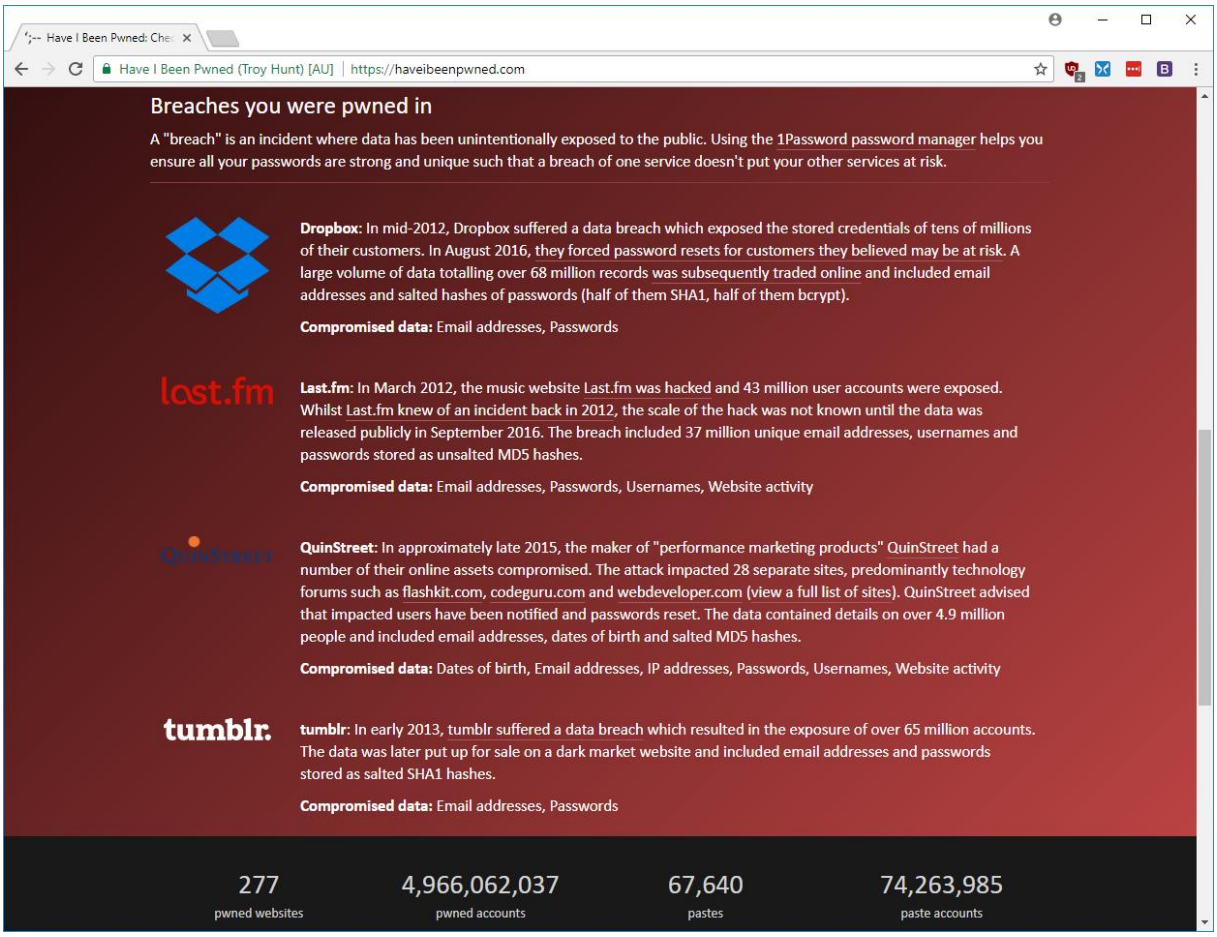
Današnji korisnici računala koriste sve veći broj mrežnih servisa kao što su servisi elektroničke pošte, društvene mreže i servisi za kupovinu putem interneta. Za pristup svom korisničkom računu na takvim servisima, korisnici najčešće moraju koristiti kombinaciju korisničkog imena (ili adrese e-pošte) te lozinke.

Kako ne bi morali pamtiti brojne lozinke, korisnici često koriste istu lozinku za sve servise. Nažalost, to predstavlja ozbiljan sigurnosni rizik. U tom slučaju, ako napadač ukrade lozinku korisnika na jednom servisu, može ju iskoristiti i za pristup drugim servisima.

Have I Been Pwned je Web servis sigurnosnog stručnjaka Troya Hunta koji korisnicima može prikazati stvarnu ozbiljnost ovog sigurnosnog rizika. *Have I Been Pwned* sadrži bazu podataka s informacijama o milijunima korisničkih računa koji su ukradeni u napadima na stotine različitih mrežnih servisa.



Na službenoj stranici servisa korisnik može upisati korisničko ime ili adresu e-pošte s kojom se registrirao na neki mrežni servis. Zatim, pritiskom na tipku „*pwned?*“, servis će ispisati popis njemu poznatih krađa podataka u kojima se nalazio i korisnički račun s upisanim korisničkim imenom odnosno adresom e-pošte.



U gornjem primjeru moguće je vidjeti kako i poznati servisi koji ulažu značajne resurse u sigurnost nisu sigurni od krađe korisničkih podataka.

Nažalost, ni korištenje različitih lozinki za svaki servis nije samo po sebi dovoljno. Ako korištene lozinke nisu dovoljno složene, napadač može dobiti pristup korisnikovom računu napadom uzastopnim pogađanjem (eng. *brute-force attack*). Iz tog razloga, osim što bi lozinke trebale biti različite za različite servise, one bi trebale i biti složene. Drugim riječima, one bi trebale biti dugačke (desetak ili više znakova), trebale bi sadržavati različite vrste znakova (velika slova, mala slova, znamenke…) i slično.

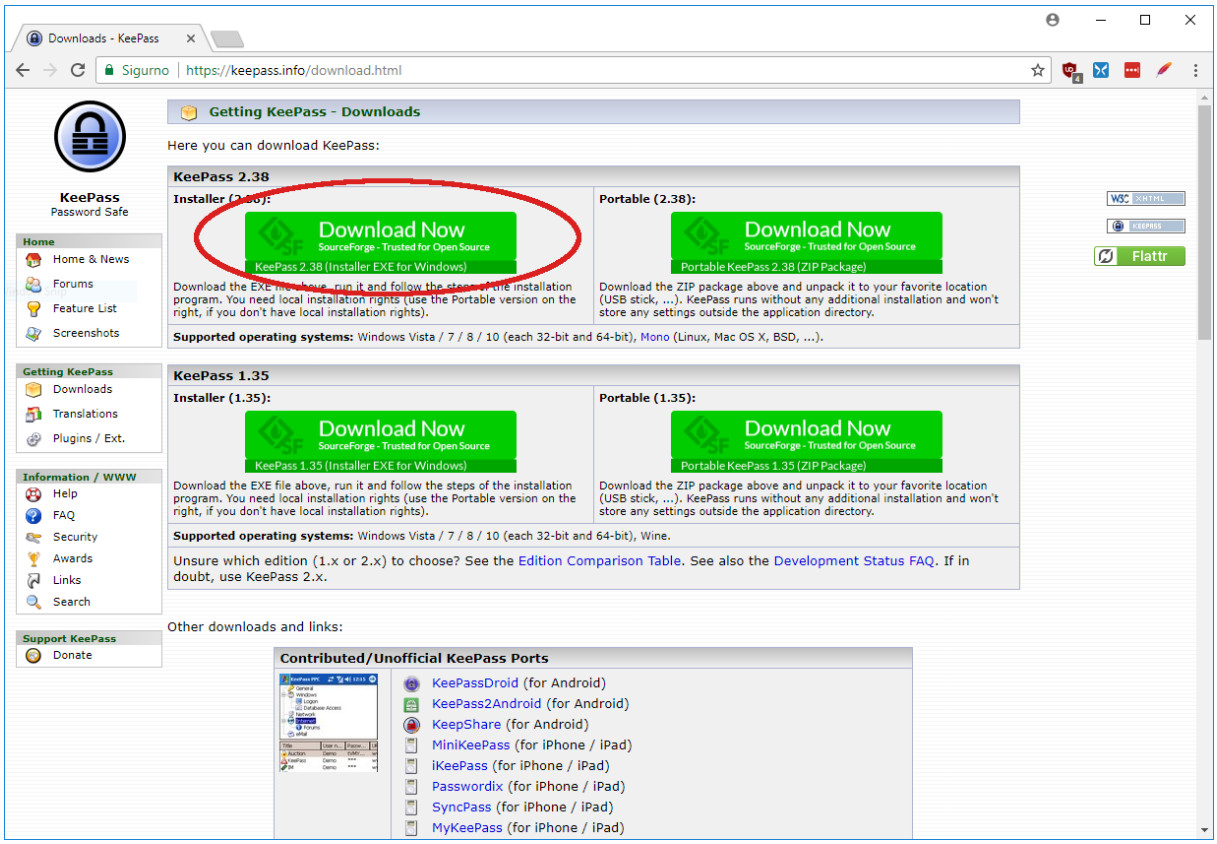
Kako bi se doskočilo problemu pamćenja većeg broja složenih lozinki, koriste se tzv. upravitelji lozinkama (engl. *password managers*) koji omogućavaju generiranje i pohranu većeg broja složenih lozinki u šifriranom obliku. Do lozinki u izvornom obliku se dolazi poznavanjem samo jedne, glavne lozinke (engl. *master password*) koja omogućava dešifriranje ostalih lozinki. Na taj način, krajnji korisnik mora zapamtiti samo jednu, glavnu lozinku, ali može koristiti različite, složene lozinke za različite servise.

Jedan od takvih upravitelja lozinkama je i KeePass, alat otvorenog koda dostupan na osobnim računalima sa sustavima Windows, Linux i macOS. KeePass nudi jednostavno sučelje za upravljanje podacima korisničkih računa uz visoku razinu sigurnosti. U ovom dokumentu bit će objašnjen postupak instalacije te uobičajeno korištenje alata KeePass.

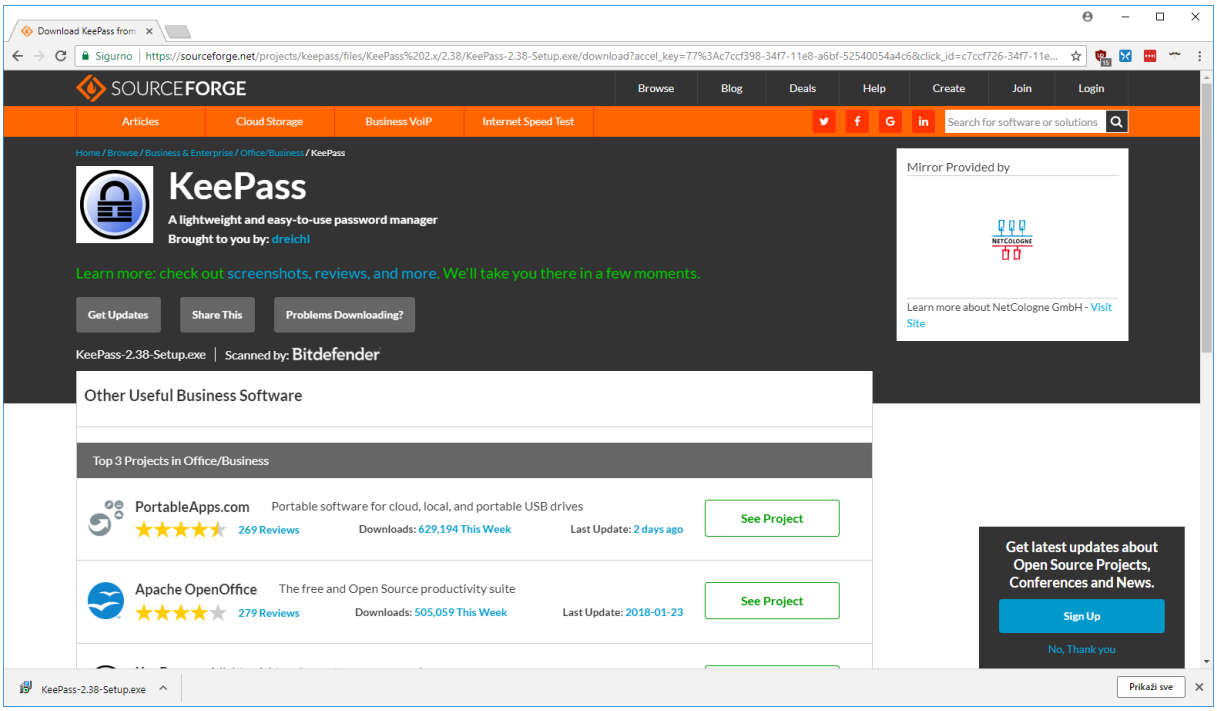
2 Instalacija alata KeePass

Instalacija će biti opisana za operacijski sustav Windows 10, no postupak instalacije je sličan i na ostalim podržanim operacijskim sustavima. Postoje dvije inačice programa KeePass koje se paralelno razvijaju: inačica 1.x i inačica 2.x. Inačica 2.x nije kompatibilna s inačicom 1.x, no nudi veći broj mogućnosti i preporučena je za nove korisnike. Na starijim sustavima na kojima se inačica 2.x ne može pokrenuti, moguće je koristiti inačicu 1.x. U ovom dokumentu koristit će se inačica 2.38, izdana 9. siječnja 2018.

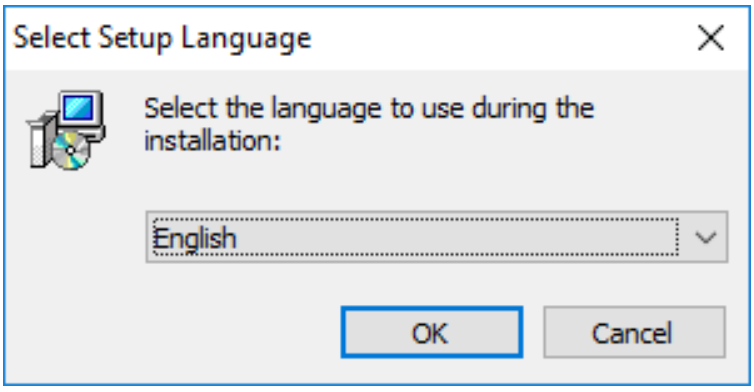
Poveznice za preuzimanje alata KeePass dostupne su na službenim stranicama alata. Za preuzimanje alata, potrebno je pritisnuti tipku za odgovarajuću inačicu, zaokruženu na donjoj slici.



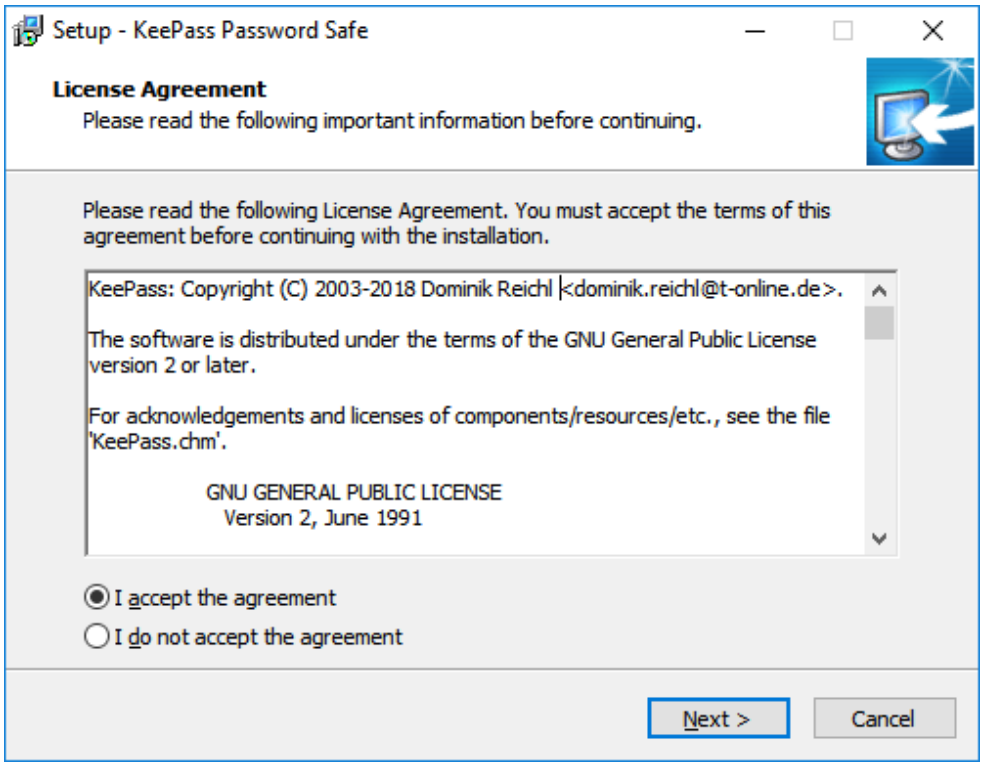
Nakon toga otvara se stranica na servisu *SourceForge*, s kojeg će se automatski skinuti instalacijska datoteka. Pokretanjem te datoteke započinje instalacijski proces.



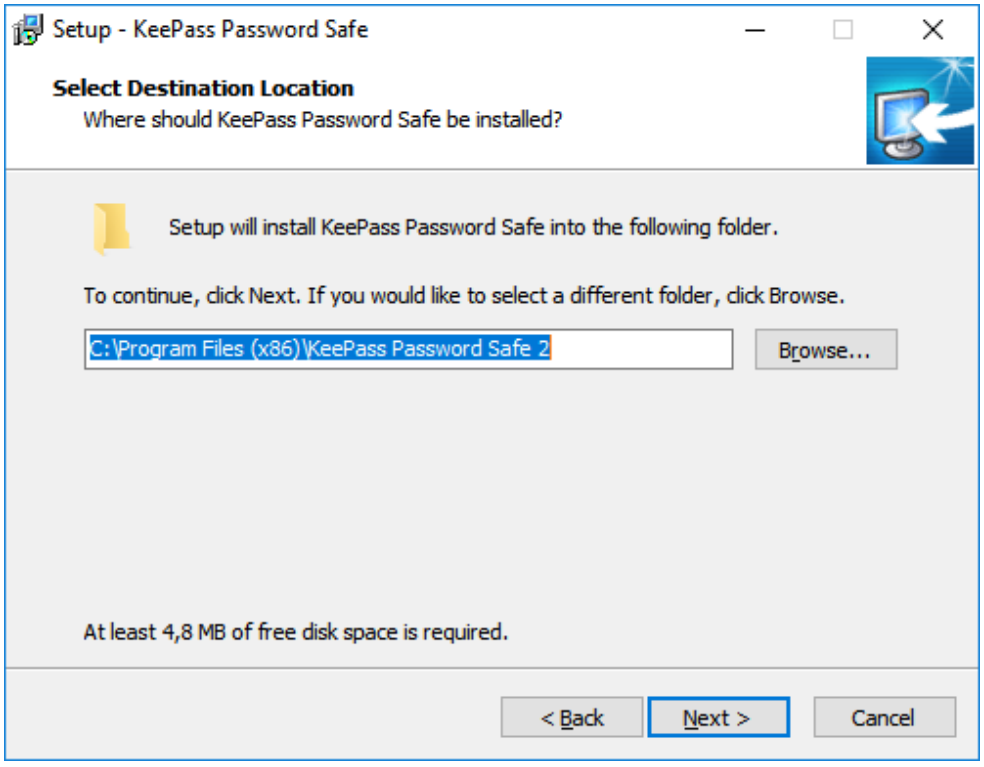
Nakon pokretanja izvršne datoteke, u prvom koraku instalacijskog procesa alata KeePass potrebno je potvrditi engleski jezik kao jezik instalacije pritiskom na tipku ***OK***.



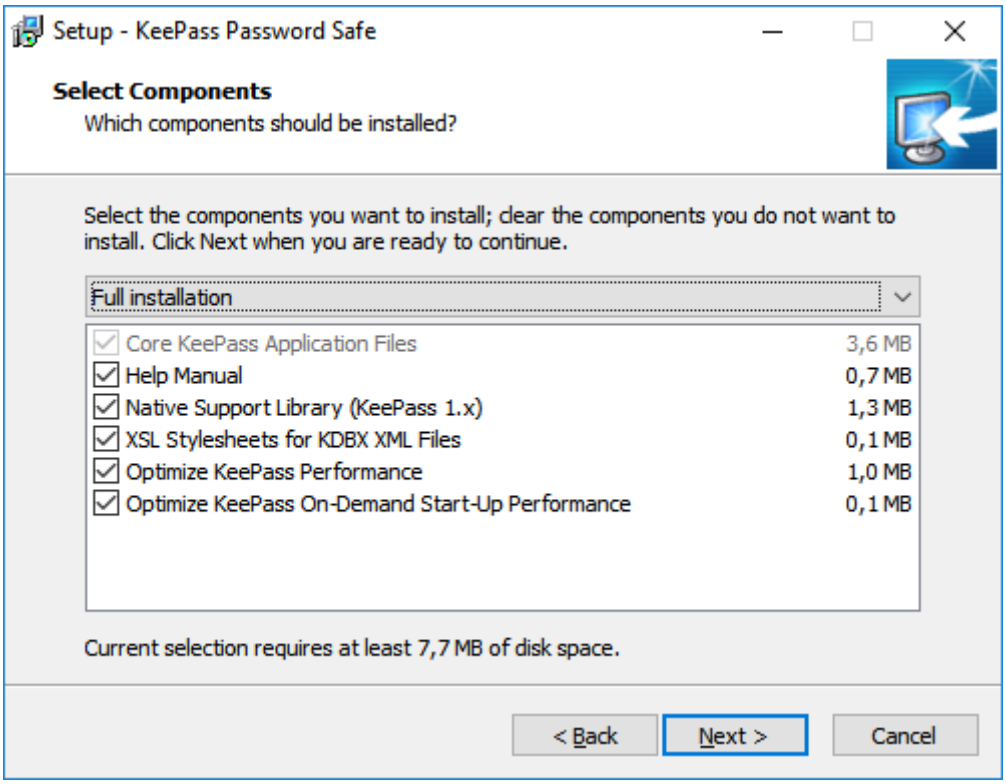
Odabirom *I accept the agreement* kako bi se prihvatila licenca alata KeePass te pritiskom na tipku ***Next*** prelazi se na sljedeći korak.



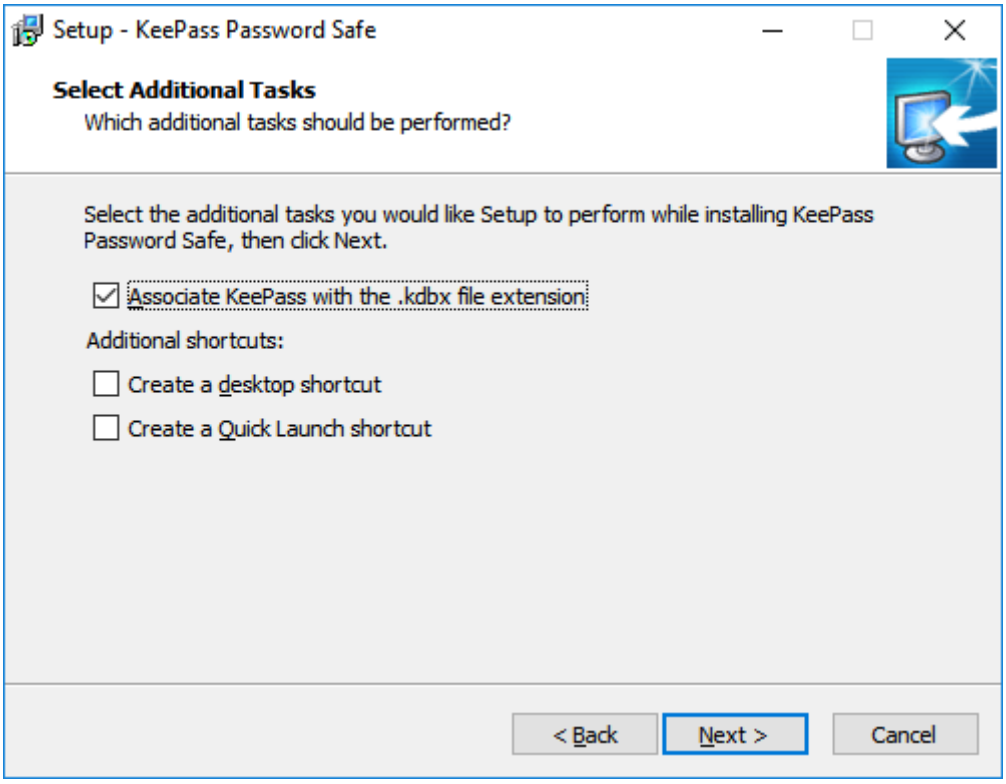
Sada je potrebno odabrati direktorij u kojem će se nalaziti datoteke alata KeePass. U ovom primjeru ostavljen je direktorij zadan u instalacijskom procesu. Nakon eventualnog mijenjanja instalacijskog direktorija pritiskom na ***Next*** prelazi se na sljedeći korak.



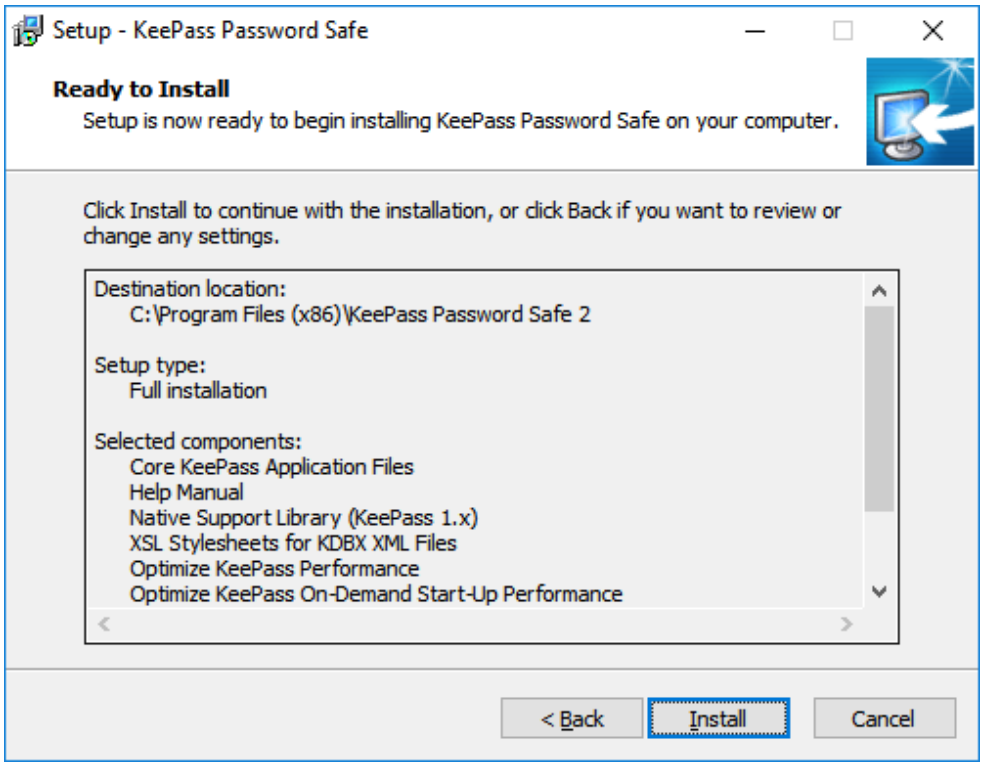
U ovom koraku moguće je odabrati dijelove alata KeePass koji će se instalirati. Preporuča se odabir svih dijelova, tj. bez mijenjanja postavki pritisnuti tipku ***Next*** za sljedeći korak.



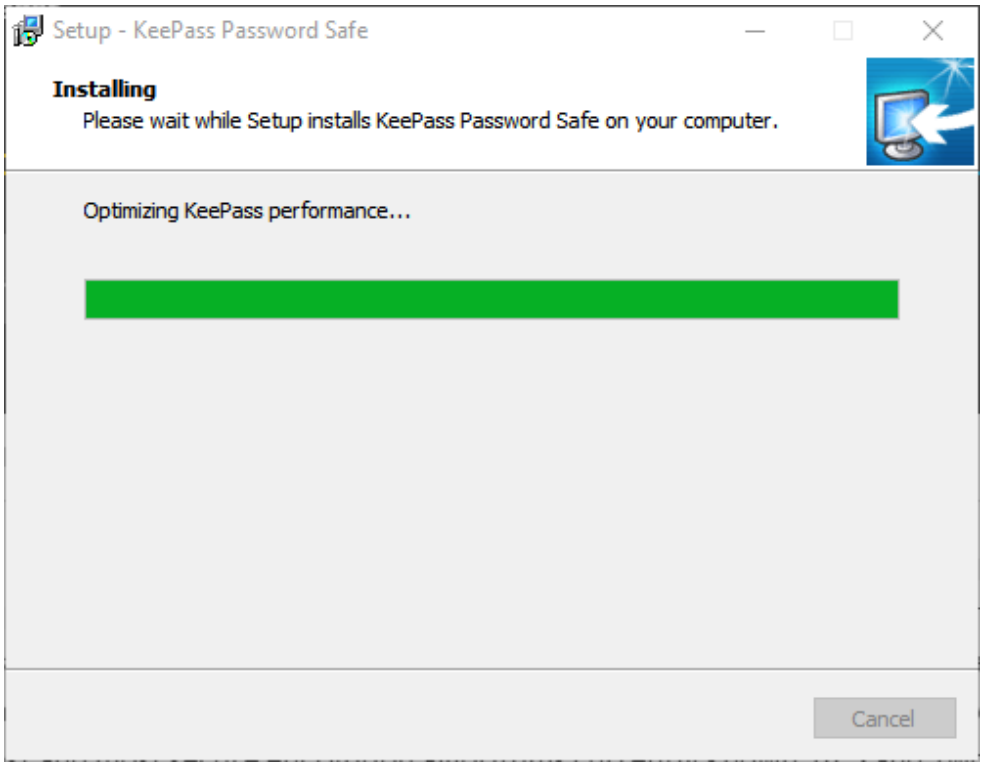
Sada je moguće odabrati postavljanje ikone na radnu površinu ili na traku za brzo pokretanje programa. Nakon ovih neobaveznih postavki potrebno je pritisnuti tipku ***Next***.



Zatim, moguće je provjeriti prethodno odabrane postavke te pritisnuti na tipku ***Install*** kako bi započela instalacija alata KeePass.

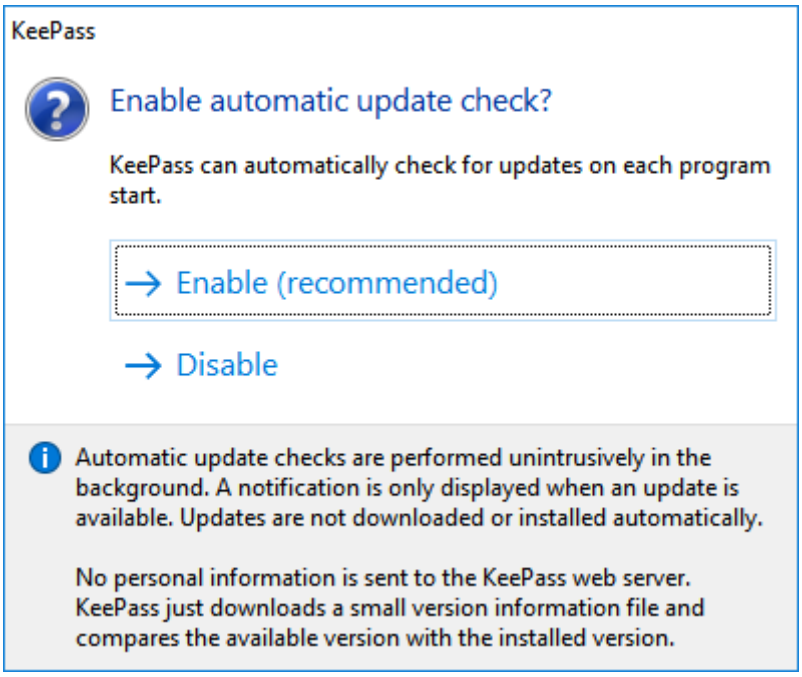


Sada započinje instalacija alata KeePass koja u pravilu ne traje dugo:



Nakon što je završila instalacija datoteka, pokazuje se zadnji korak u instalacijskom procesu koji se izvršava pritiskom na ***Finish***.

Pri prvom pokretanju alata KeePass pojavljuje se prozor u kojem je potrebno omogućiti ili onemogućiti automatsko provjeravanje dostupnosti novih inačica programa. Preporučljivo je odabirom ***Enable*** uključiti automatsko provjeravanje kako bi se KeePass držao ažurnim i sigurnim.

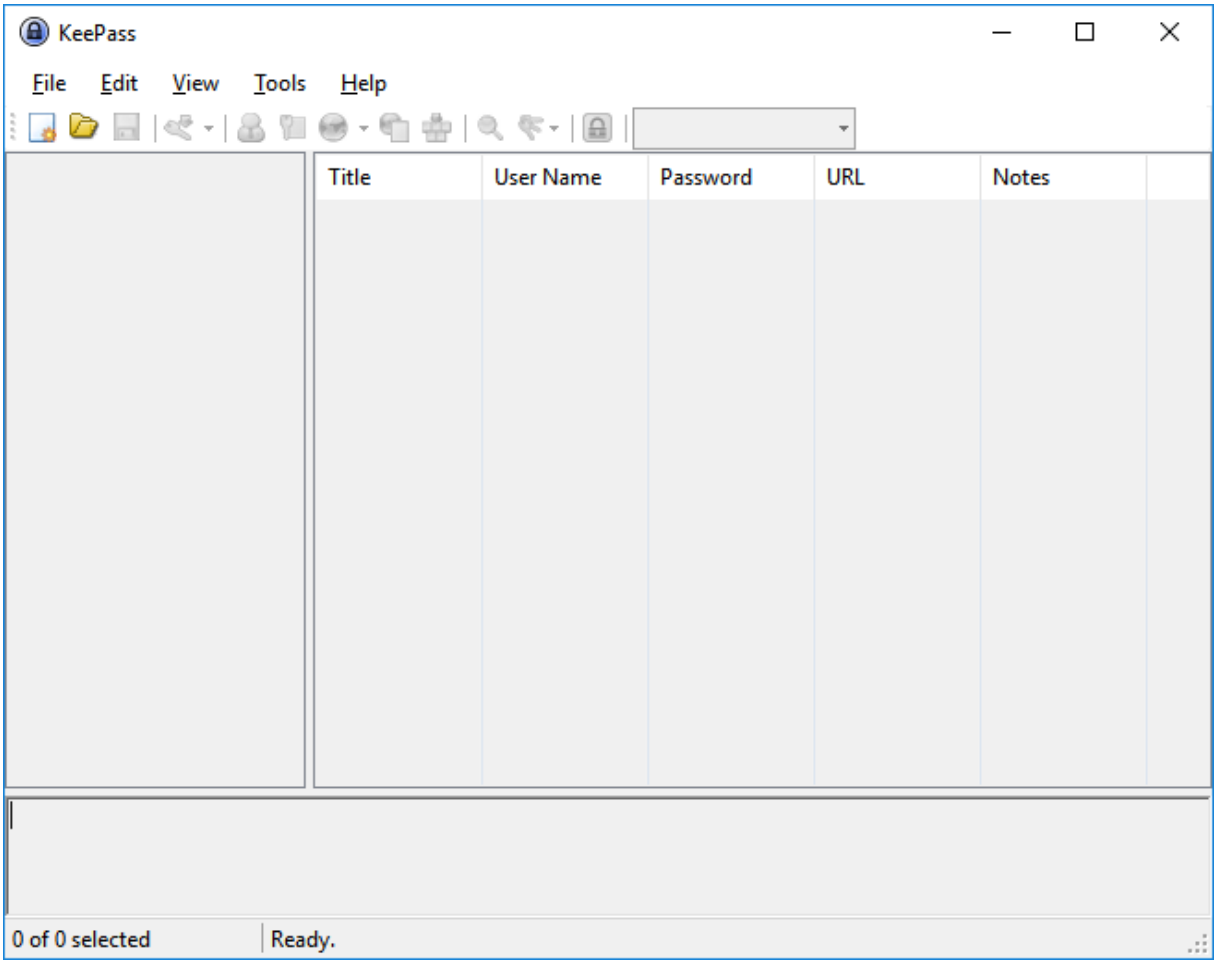


3 Korištenje alata KeePass

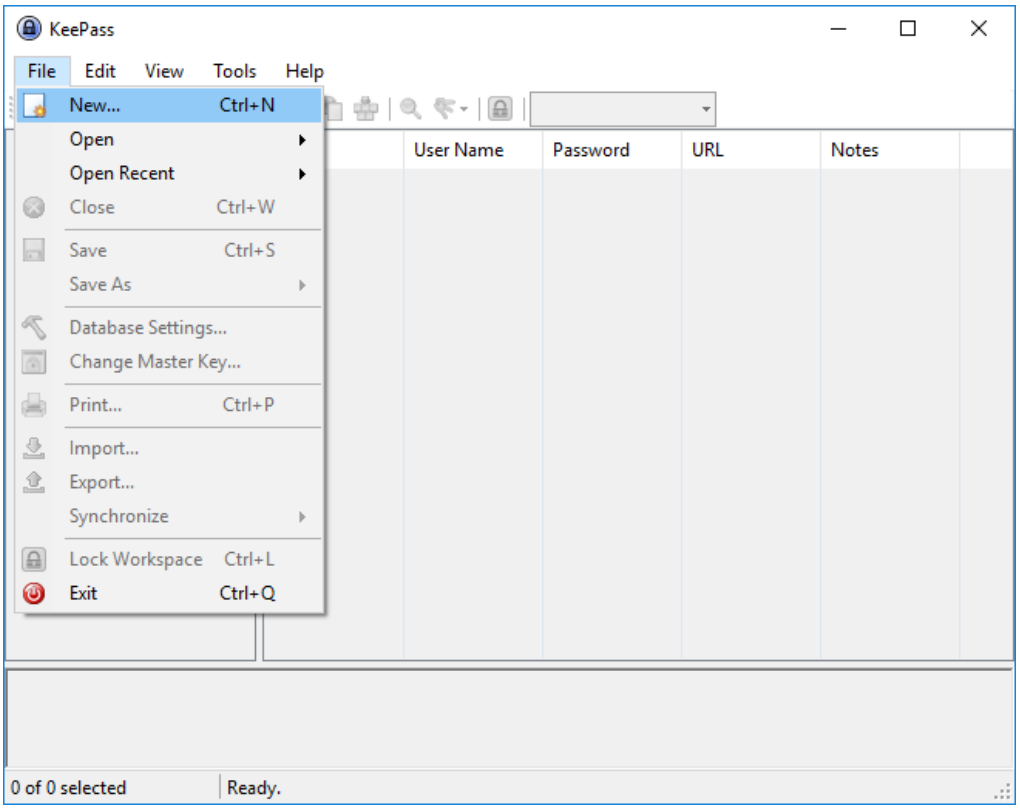
U ovom poglavlju bit će opisane uobičajene radnje korisnika u alatu KeePass: stvaranje baze podataka u koju se spremaju unosi (podaci o korisničkim računima, npr. korisničko ime i lozinka) te dodavanje i brisanje takvih unosa.

3.1 Stvaranje baze podataka

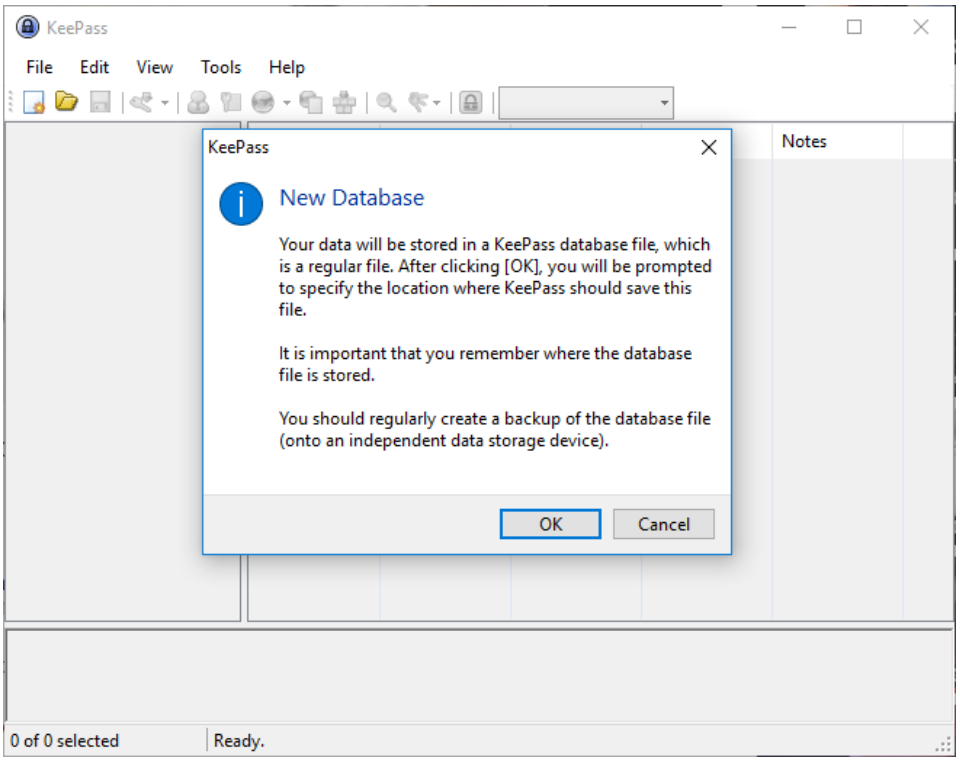
Prije dodavanja unosa u KeePass potrebno je stvoriti bazu podataka. Baza podataka bit će šifrirana te će se podacima u njoj moći pristupati isključivo korištenjem glavne lozinke (eng. *master password*). Na donjoj slici prikazan je izgled početnog zaslona alata KeePass prije stvaranja baze podataka.



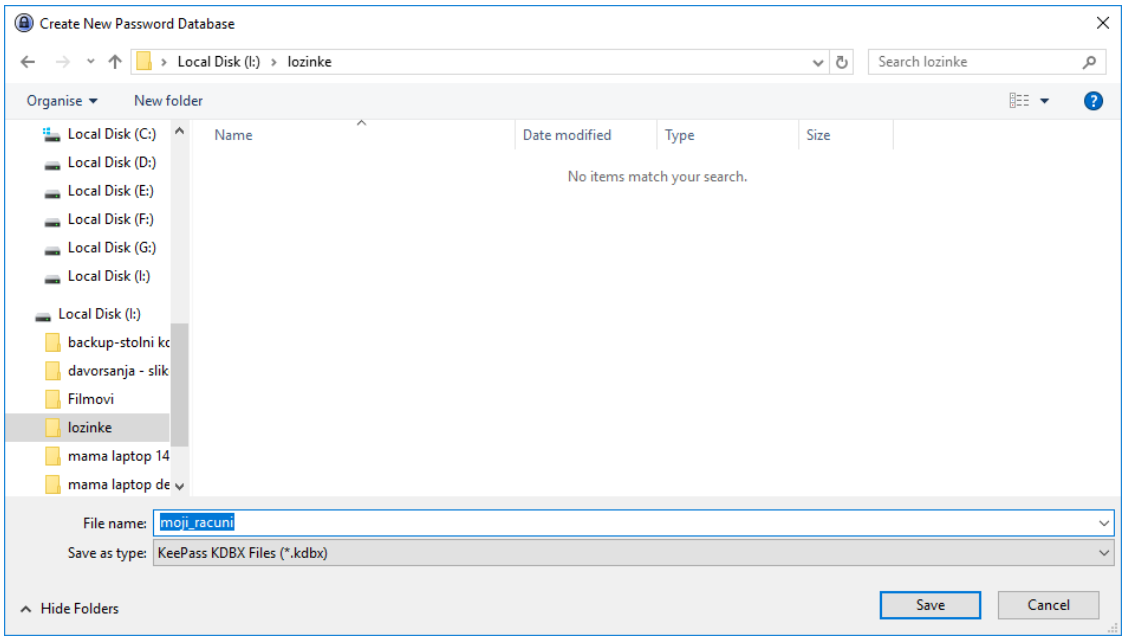
Da bi se stvorila baza podatka potrebno je odabrati ***File*** u glavnom izborniku te pritisnuti na ***New***.



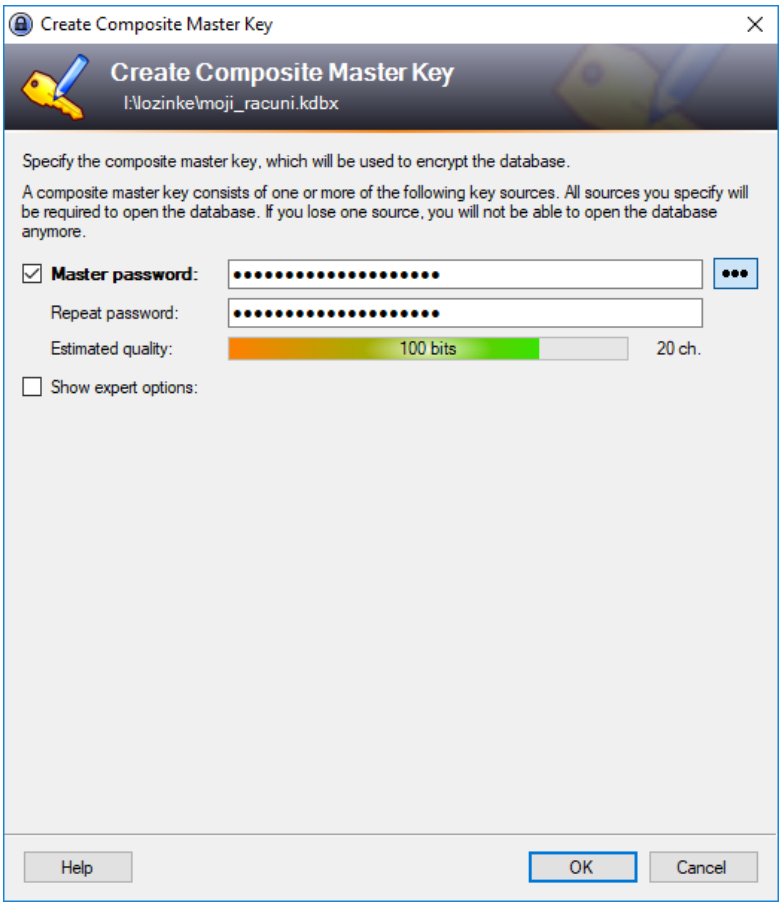
Sada se prikazuje prozor u kojem se korisnika obavještava kako će se stvoriti datoteka za bazu podataka. Treba zapamtiti gdje se ona nalazi te redovito stvarati sigurnosne kopije (engl. *backup*) kako se ne bi izgubili podaci o korisničkim računima u slučaju neke greške ili kvara na računalu. Pritiskom na ***OK*** prelazi se na sljedeći korak.



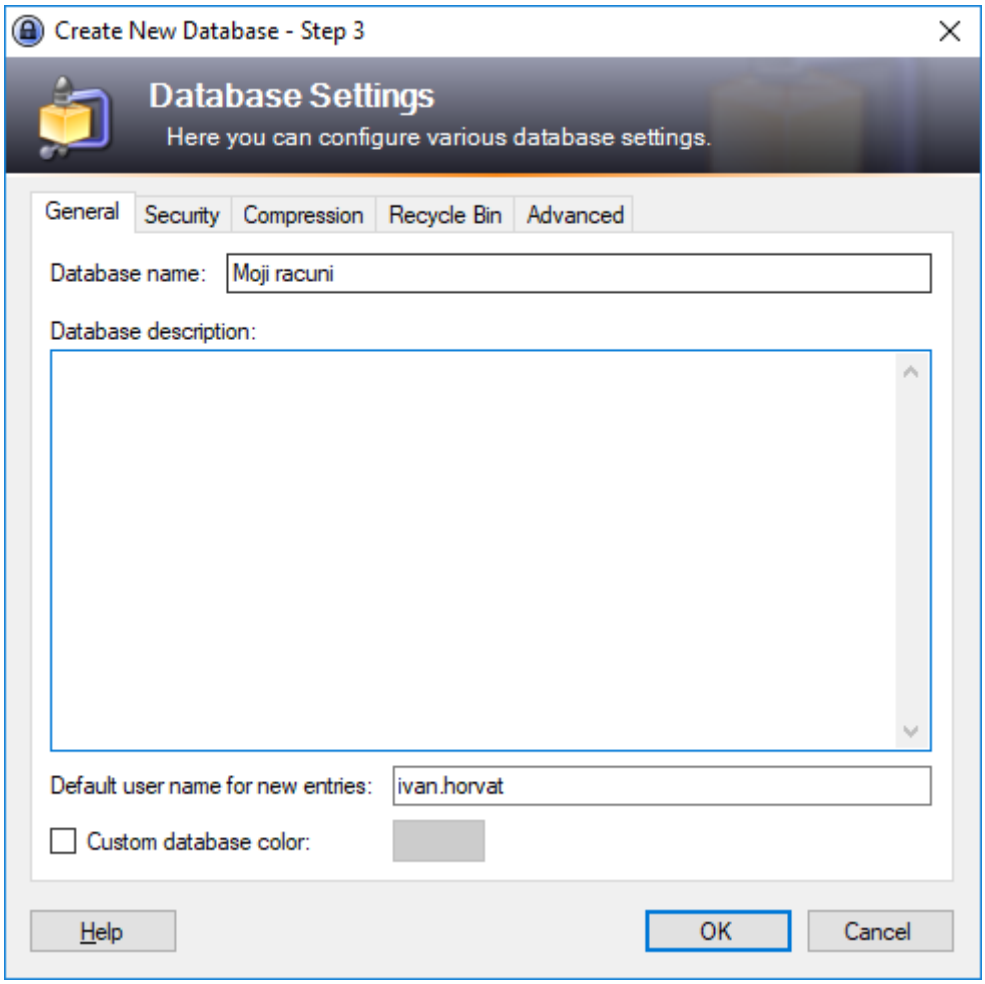
U ovom koraku potrebno je odabrati ime datoteke baze podataka te direktorij u koji će se ona spremiti. Nakon odabira pogodnog imena i mjesta datoteke, klikom na ***Save*** prelazi se na sljedeći korak.



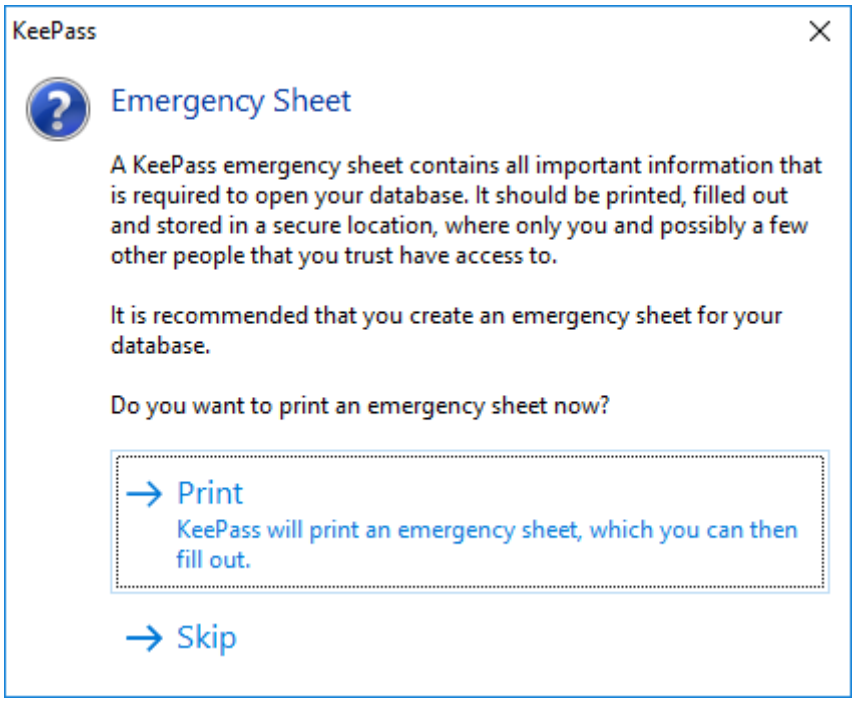
Pojavljuje se novi prozor u kojem je potrebno odabrati glavnu lozinku koja će se koristiti za šifriranje, odnosno dešifriranje baze podataka. Potrebno je odabrati složenu lozinku i time osigurati da potencijalni napadač koji dođe u posjed šifrirane baze podataka ne može bazu dešifrirati. Nakon upisivanja i potvrde lozinke, potrebno je pritisnuti ***OK*** za sljedeći korak.



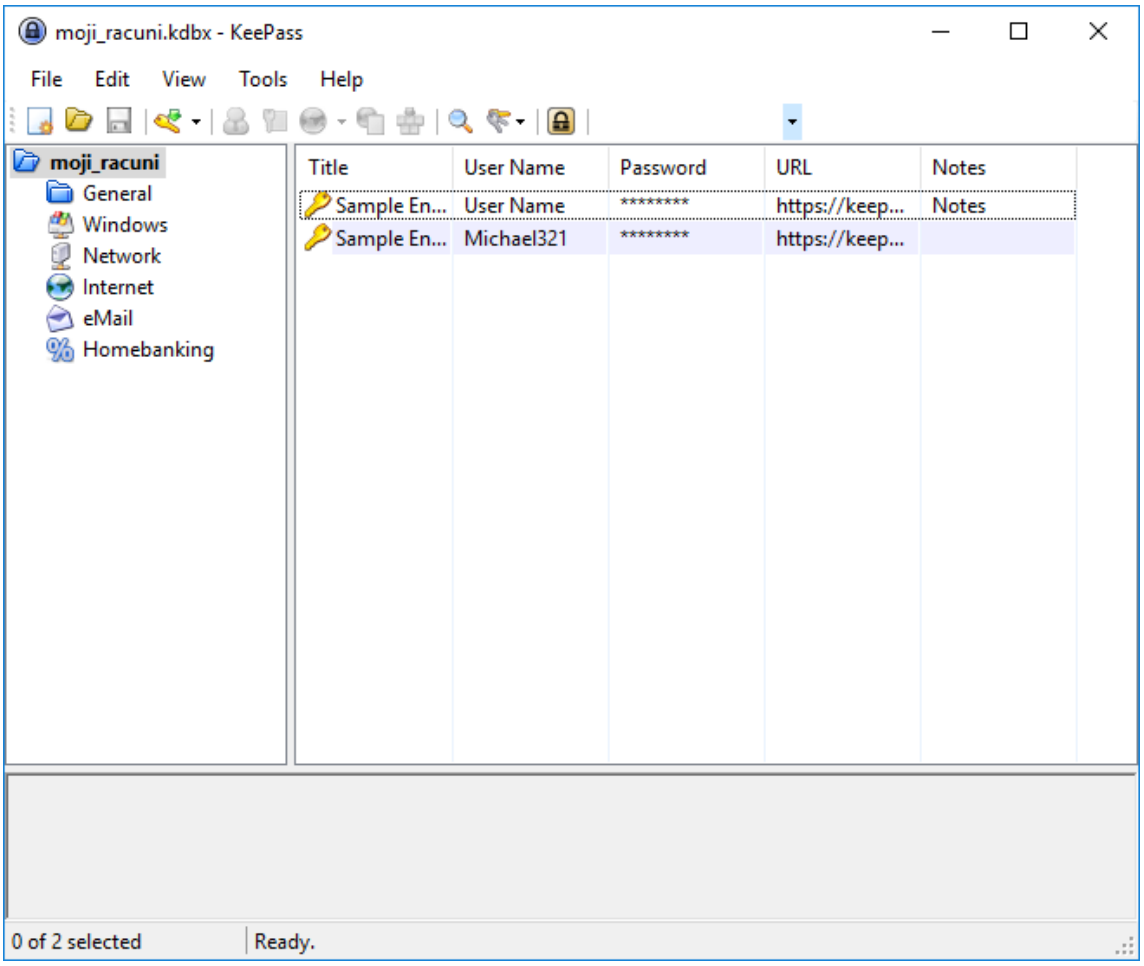
U ovom koraku moguće je mijenjati postavke baze podataka. U karticama za sigurnost (*Security)* i kompresiju (*Compression*) zadane postavke su dovoljno dobre, te ih nije potrebno mijenjati. U početnoj kartici ovog prozora (*General*) moguće je imenovati bazu podataka, dati joj opis te postaviti korisničko ime koje će automatski biti zadano pri stvaranju novog unosa. Kako bi se to korisničko ime postavilo potrebno ga je upisati u polje označeno s *Default user name for new entries*. U ovom primjeru postavljeno je korisničko ime *ivan.horvat.*



Gubljenjem datoteke baze podataka ili njene lozinke gubi se i pristup upisanim korisničkim računima što može predstavljati veliki problem. Kako bi se to spriječilo, KeePass preporučuje i omogućuje automatsko generiranje i ispisivanje obrasca za hitne slučajeve (eng. *Emergency sheet*). Na njemu se nalaze polja u koja korisnik može upisati lozinku baze podataka te mjesta na kojima je njena datoteka pohranjena (uključujući sigurnosne kopije datoteke). Na sljedećoj stranici prikazana je slika prozora u kojem je moguće odabrati ispis klikom na ***Print*** ili preskakanje ovog koraka klikom na ***Skip***.

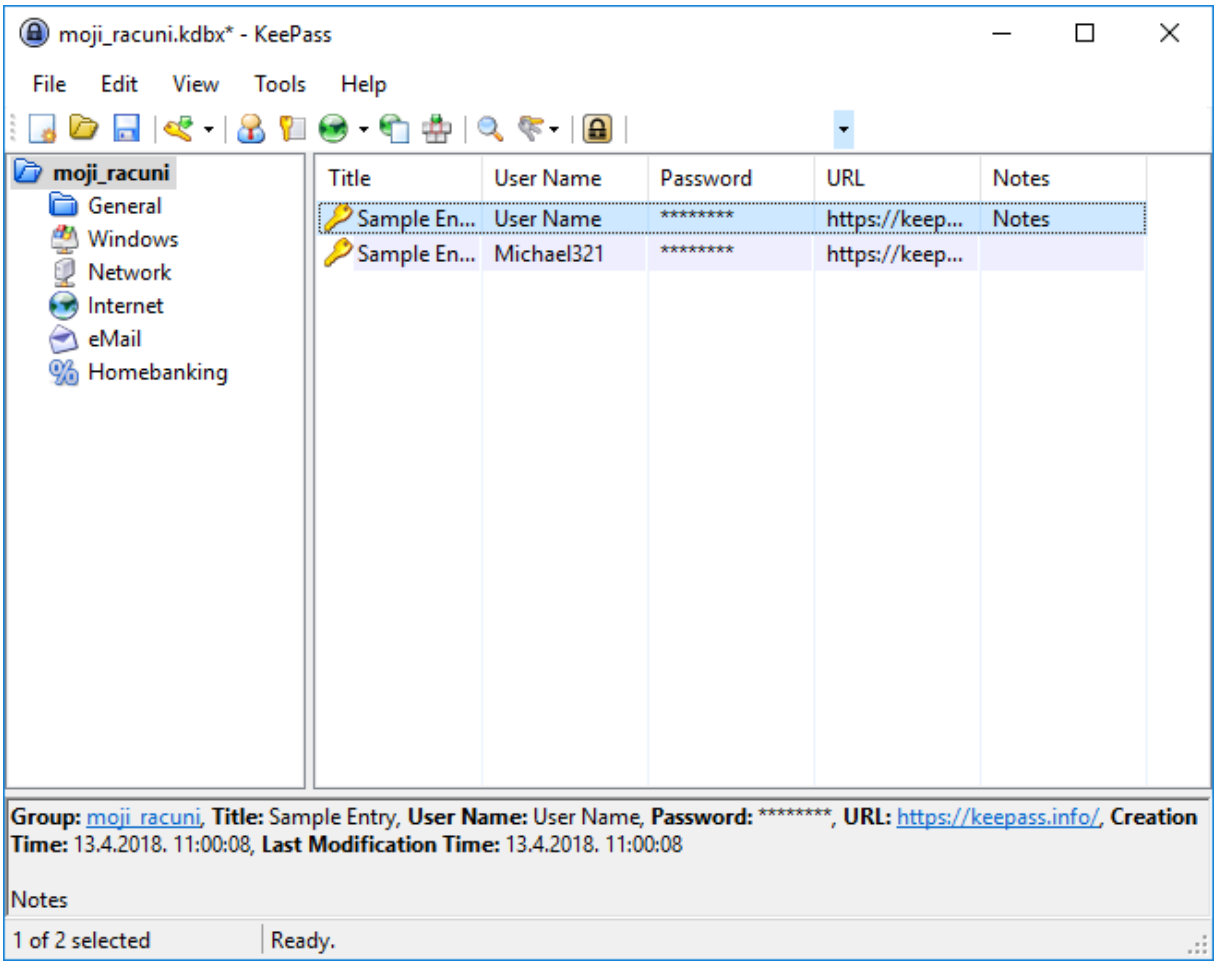


Nakon ovog koraka otvara se prozor s pregledom baze podataka, prikazan na donjoj slici. KeePass je automatski stvorio dva unosa s primjerima korisničkih podataka:



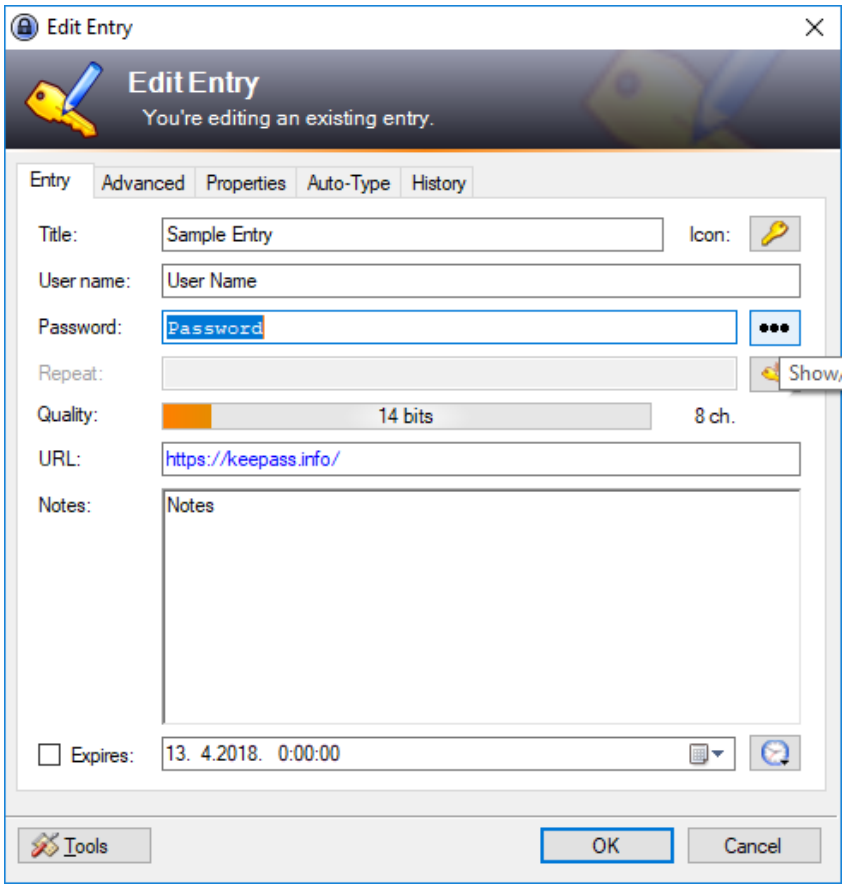
3.2 Upravljanje podacima korisničkih računa

Lijevim klikom miša na unos koji odgovara korisničkom računu moguće je u donjem dijelu prozora vidjeti podatke korisničkog računa:

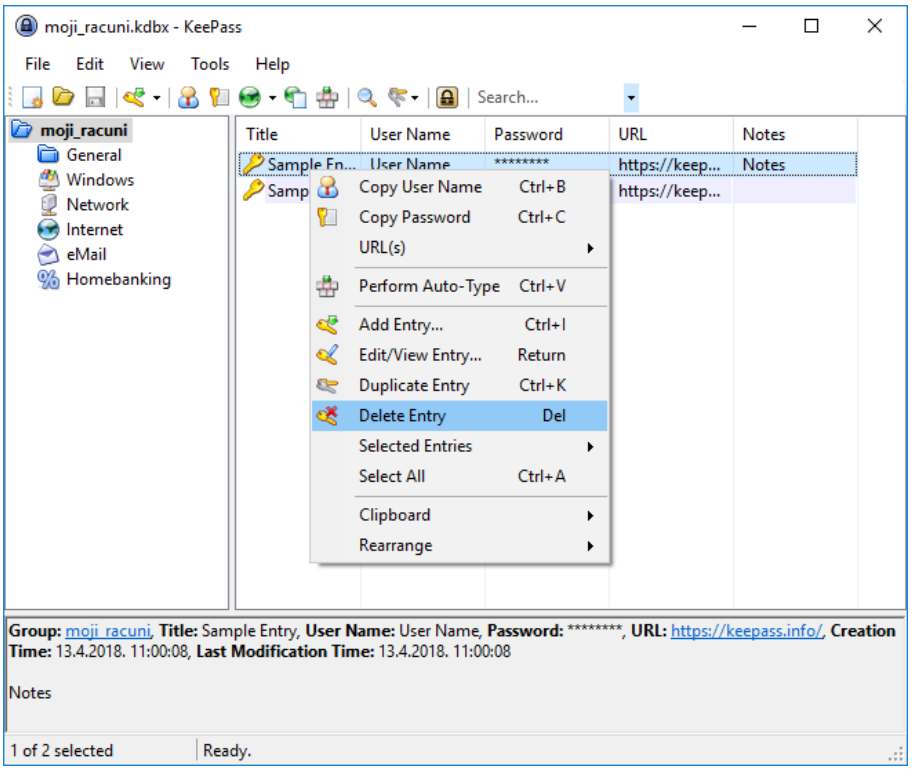


Iz sigurnosnih razloga lozinka nije prikazana u čitljivom obliku, već je sakrivena (prikazana zvjezdicama). Dvoklikom na polje u kojem se nalazi sakrivena lozinka, njen sadržaj kopira se u međuspremnik (eng. *clipboard*) operacijskog sustava te se iz njega automatski briše nakon 12 sekundi. Na isti način moguće je kopirati korisničko ime u međuspremnik operacijskog sustava. Prije nego što se automatski izbriše iz međuspremnika, lozinku ili korisničko ime moguće je kopirati u područje za njihov unos, primjerice na Web stranici za prijavu u neki sustav. Lozinku je također moguće vidjeti i promijeniti odabirom odgovarajućeg unosa te pritiskom na tipku *Enter* na tipkovnici ili desnim klikom miša na unos te pritiskom na ***Edit/View Entery***. Tada se otvara prozor, prikazan na slici niže, u kojem je moguće vidjeti i mijenjati podatke korisničkog računa.

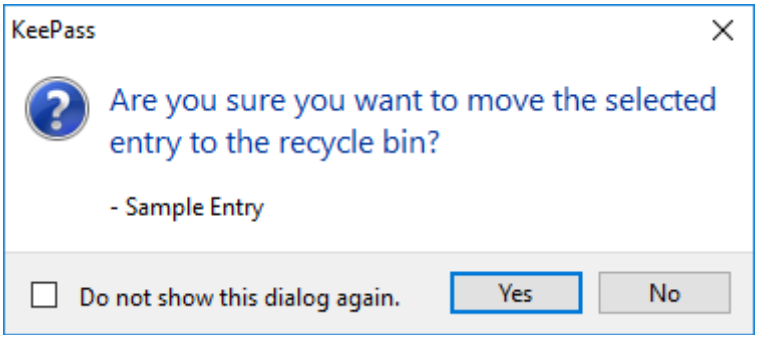
Za prikaz lozinke u izvornom obliku potrebno je pritisnuti ikonu s tri točke:



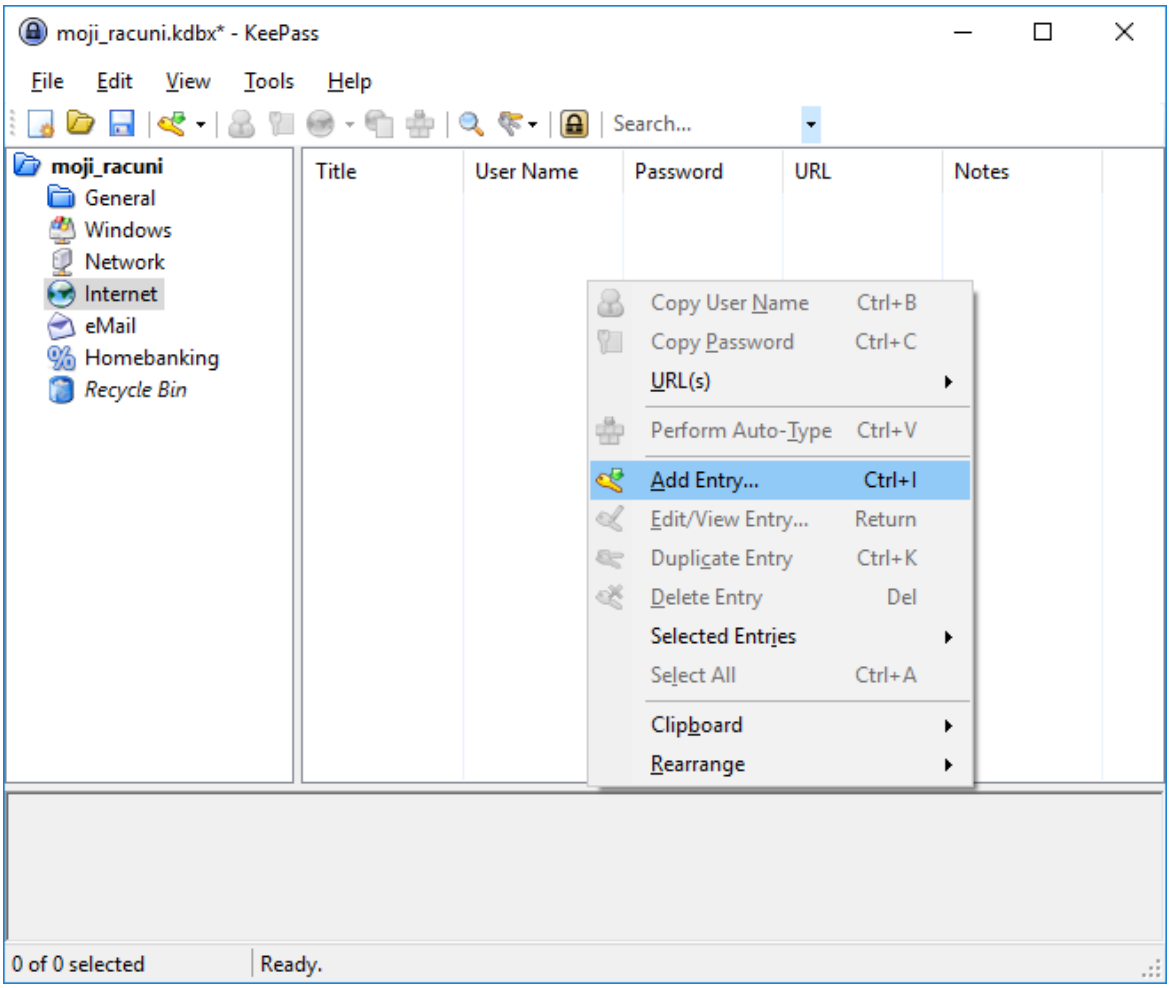
Brisanje unosa iz baze podataka moguće je ostvariti desnim klikom na njega, te odabirom ***Delete Entry:***



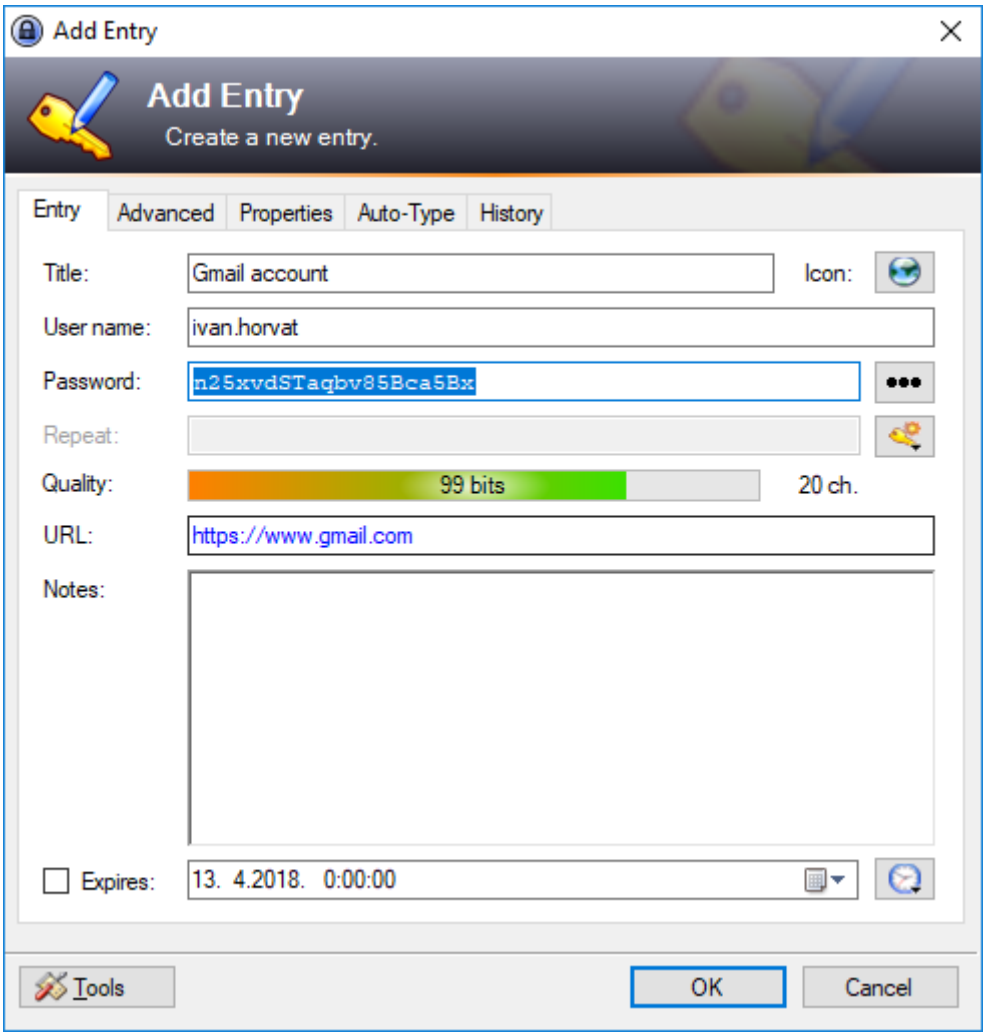
Nakon toga potrebno je potvrditi brisanje pritiskom na ***OK***. U ovom primjeru obrisana su dva automatski generirana unosa.



Kako bi unosi bili bolje organizirani, moguće ih je pohraniti u grupe, vidljive u lijevom dijelu glavnog prozora. U ovom primjeru bit će dodan unos za Web stranicu pa će zato biti odabrana grupa *Internet.* Kako bi se stvorio novi unos, u glavnom izborniku glavnog prozora potrebno je odabrati ***Edit*** pa zatim ***Add Entry***.



Sada se otvara prozor u kojem je moguće upisati ime unosa (*Title*), korisničko ime (*User name*), lozinku (*Password*), URL na kojem se nalazi stranica za prijavu na servis (*URL*), dodatne bilješke (*Notes*) te je moguće postaviti i datum kada podaci za korisnički račun ističu.



Lozinka je automatski generirana te sastoji se od 20 znakova, uključujući mala i velika slova engleske abecede te znamenke. Pritiskom na ikonu žutog ključa moguće je promijeniti duljinu lozinke i vrste znakova koji se koriste pri njenom generiranju. Ovakva lozinka dovoljno je sigurna te, ako servis prihvaća lozinku u tom obliku, zadane postavke generiranja lozinke nije potrebno mijenjati. Pritiskom na ***OK*** unos postaje dostupan u alatu KeePass.

Sve izmjene u bazi podataka treba sačuvati prije izlaska iz alata KeePass. To se može ostvariti pritiskom na tipke **Ctrl** i **S** na tipkovnici ili odabirom ***File*** u glavnom izborniku te zatim pritiskom na ***Save***.

3.3 Automatsko upisivanje podataka korisnika

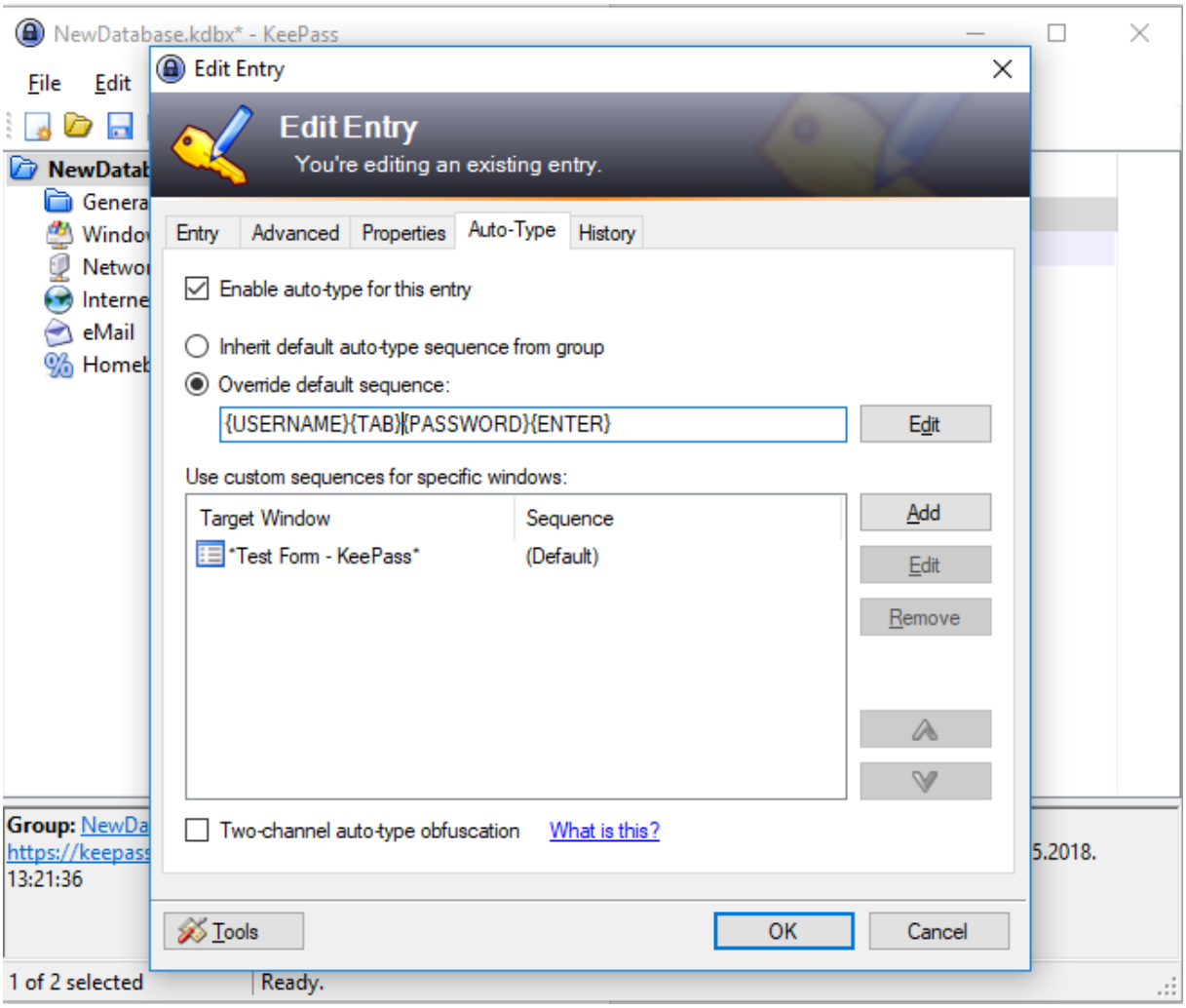
Kako bi se olakšao unos korisničkog imena i lozinke, KeePass nudi ***Auto-Type*** – funkcionalnost automatskog upisa podataka. Pomoću te funkcionalnost moguće je zadati naredbu alatu KeePass da automatski upiše korisničko ime i lozinku u obrazac na Web stranici, u prozor programa za čitanje e-pošte ili slično.

Po pretpostavljenim postavkama, *Auto-Type* funkcionalnost upisuje korisničko ime, zatim tipku Tab, pa lozinku i konačno tipku Enter. Ovaj slijed radnji odgovara obrascima za prijavu na velikom broju Web stranica i programa općenito, no za neke ipak mora biti izmijenjen. To je moguće ostvariti desnim klikom na unos, zatim na *Edit/View entry* te u kartici *Auto-Type* odabrati *Override default sequence* i upisati željeni slijed.

U istom prozoru, prilikom konfiguracije *Auto-Type* funkcionalnosti, preporuča se uključivanje postavke ***Two-channel auto-type obfuscation***. Time se unos korisničkog imena i lozinke ne radi isključivo simulacijom upisivanja preko tipkovnice, već se dodatno koristi i *clipboard* međuspremnik operacijskog sustava. Ovakva tehnika automatskog upisivanja korisničkih podataka služi kao prepreka potencijalno zlonamjernom softveru na korisnikovom računalu koje pokušava otkriti lozinke špijuniranjem pritisnutih tipka i/ili *clipboard* međuspremnika.

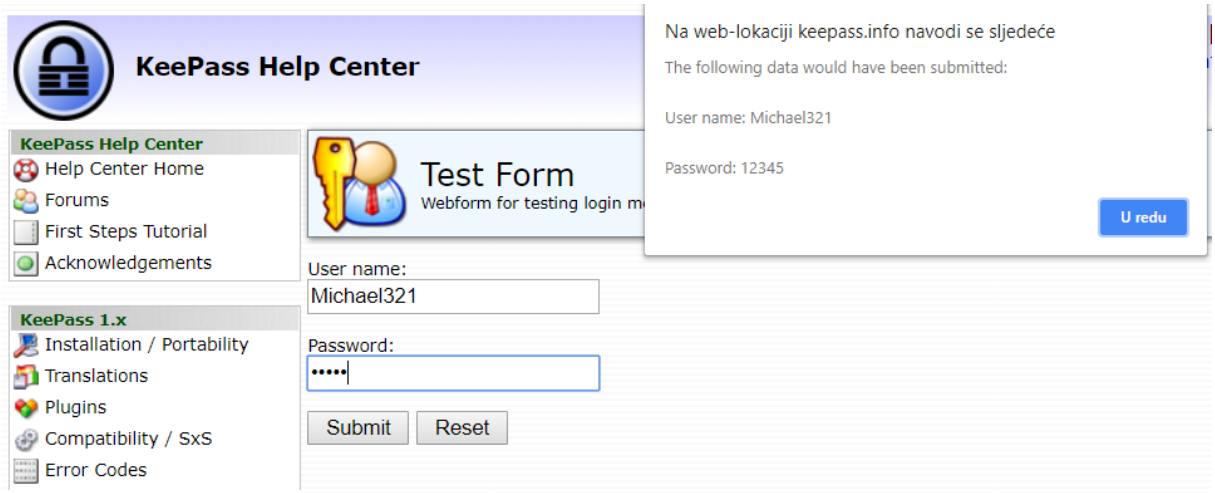
Također je u istom prozoru korisno definirati ciljne prozore, tj. prozore na kojima se korisnički podaci trebaju moći automatski upisati. To je moguće konfigurirati pritiskom na tipku ***Add*** te upisom naslova prozora u ***Target window*** polje. Ako je željeni prozor već otvoren, nije potrebno ručno upisivati njegov naslov, već ga je moguće odabrati iz padajućeg izbornika. Unos naslova je fleksibilan – podržan je i poseban znak „*“ kojim se označava bilo koji niz znakova (eng. *wildcard*), a za naprednije korisnike podržani su i regularni izrazi (eng. *regular expressions*).

Dodatna pojašnjenja te razne mogućnosti vezane za upis slijeda radnji, konfiguraciju ciljnih prozora te ostale *Auto-Type* postavke moguće je pronaći na pripadajućoj Web stranici dokumentacije alata KeePass.



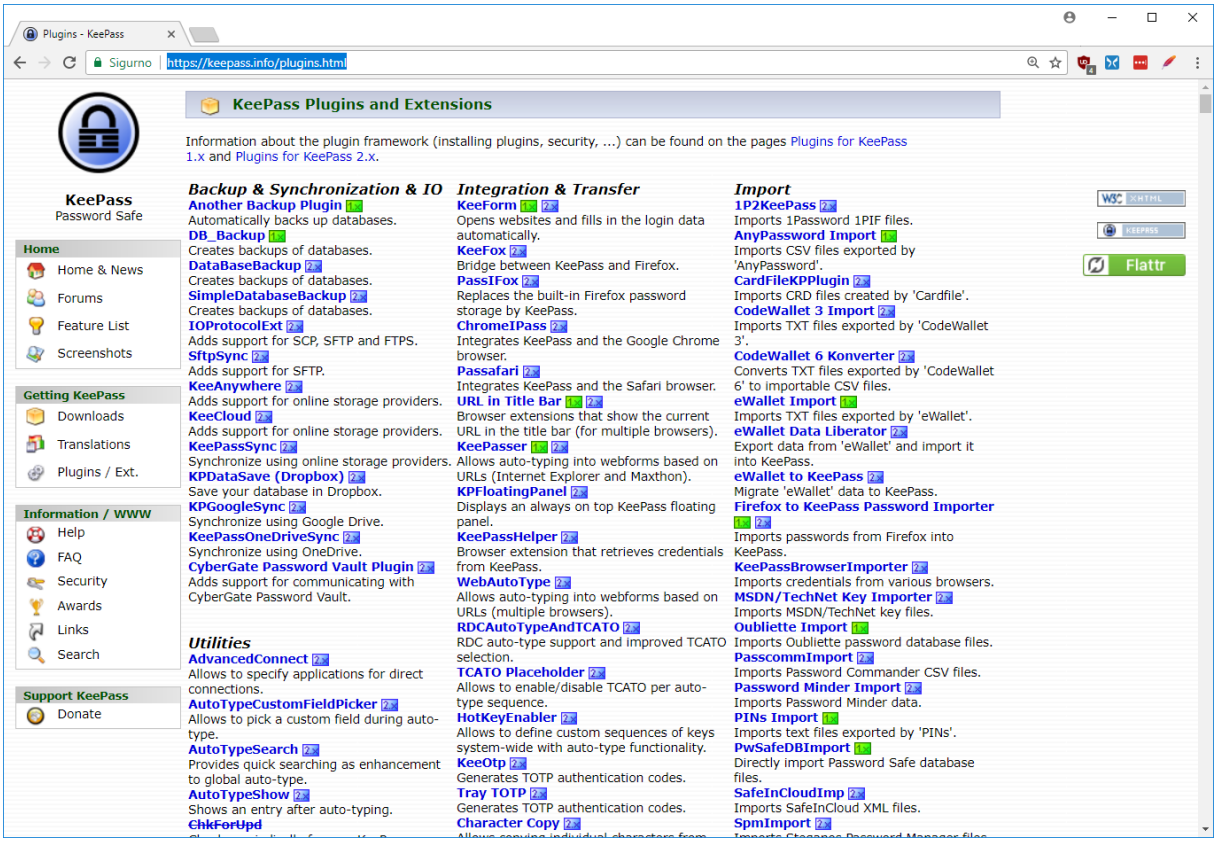
Na Web stranici alata KeePass nalazi se i obrazac pomoću kojeg je moguće ispitati *Auto-Type* funkcionalnost. Ukoliko je za korisničke podatke otvoreni prozor definiran kao ciljni, za automatski upis podataka dovoljno je označiti polje za korisničko ime i pritisnuti kombinaciju tipki ***Ctrl***, ***Alt*** i ***A***.

U suprotnom, potrebno je označiti polje za unos korisničkog imena te zatim otvoriti KeePass. Tada je u glavnom prozoru alata KeePass potrebno označiti odgovarajući unos pritiskom na njega. Konačno, pritiskom kombinacije tipki ***Ctrl*** i ***V*** ili desnim klikom miša na unos s podacima te odabirom ***Perform Auto-Type*** započinje automatsko upisivanje podataka korisnika. Rezultat automatskog upisivanja podataka korisnika prikazan je na slici niže.



3.4 Dodaci alatu KeePass

KeePass je moguće proširiti dodatnim funkcionalnostima koristeći dodatke (engl. *plugins*). Na ovoj poveznici nalazi se službeni popis dodataka alata KeePass:



Kao što je vidljivo na Web stranici, KeePass nudi dodatke za integraciju s raznim servisima, za stvaranje sigurnosnih kopija, za integraciju s Web preglednicima i još niz dodataka koji mijenjaju ili dodaju razne funkcionalnosti. Neki dodaci dostupni su samo za određenu inačicu (1.x ili 2.x), a neki za obje. Nakon imena dodatka nalazi se ikona koja označava s kojom inačicom se dodatak može koristiti. Inačica 2.x nudi značajno veći broj dodataka, što je također jedan od argumenata za njeno korištenje.

4 Zaključak

Kako bi korisnici osigurali pristup svojim računima na mrežnim servisima, nužno je koristiti različite, složene lozinke za svaki servis. Kako korisnik tada ne bi morao pamtiti veliki broj složenih lozinki, razvijeni su alati za rukovanje lozinkama, a jedan od najpoznatijih, KeePass, opisan je u ovom dokumentu.

Pomoću alata KeePass moguće je spremiti podatke korisničkih računa tako da budu šifrirani jednom, glavnom lozinkom. Korisnik tada mora pamtiti samo jednu lozinku, a do podataka svojih korisničkih računa dolazi korištenjem jednostavnog grafičkog sučelja.

Osim ugrađenih mogućnosti, velikim brojem dostupnih dodataka moguće je proširiti KeePass te ugraditi mogućnosti kao što su integracija s Web preglednicima i automatska izrada sigurnosnih kopija. Velika prednost alata KeePass je to što je njegov kod otvoren i što se kontinuirano razvija i nadograđuje dugi niz godina, zbog čega je i jedan od najpopularnijih alata za rukovanje lozinkama.