



LexDesk

Bezbednost, zaštita podataka
i integritet izdanja

Verzija 2.0.0

10. avgust 2026.

NBK Code · NBK Systems

Tehnički pregled zaštite za advokatske kancelarije

Sadržaj

Podaci pod kontrolom kancelarije	3
1. Lokalna baza i autonomija kancelarije	3
2. Kriptografska zaštita baze	3
3. PIN zaštita i kontrola pristupa	4
4. LexDesk Companion i dozvole uređaja	4
5. Provera integriteta aplikacije	4
6. Kriptografski potpis i bezbedne nadogradnje	4
7. Interni kriptografski žig	5
8. Dokumentovano interno testiranje	5
9. Uvid u dokumentaciju testiranja	6
10. Podrška obavezama iz propisa Republike Srbije	6
11. Granice tehničke zaštite	7
Zaključak	7
Poruka vlasnika NBK Code-a	8
Reference	8

Podaci pod kontrolom kancelarije

LexDesk V2.0.0 razvijen je kao lokalno poslovno rešenje za advokatske kancelarije koje obrađuju poverljive podatke, dokumentaciju i informacije zaštićene obavezom čuvanja advokatske tajne.

Glavna baza podataka nalazi se na računaru korisnika. NBK Code nema pozadinski pristup sadržaju predmeta, dokumentima, rezervnim kopijama niti recovery podacima kancelarije.

Zaštita se ne oslanja na jednu lozinku ili jednu bezbednosnu funkciju. LexDesk koristi više međusobno povezanih slojeva zaštite za:

- poverljivost podataka;
- kontrolu pristupa;
- integritet baze i programskih datoteka;
- bezbedno povezivanje LexDesk Companiona;
- proveru autentičnosti nadogradnji;
- oporavak podataka u kontrolisanim uslovima;
- blokiranje neproverenih ili izmenjenih izdanja.

Nijedna pojedinačna mera ne može sama da ukloni sve rizike. Zbog toga je zaštita postavljena po principu višeslojne odbrane.

1. Lokalna baza i autonomija kancelarije

Glavna LexDesk baza ostaje u lokalnom okruženju advokatske kancelarije.

Redovan rad sa predmetima, klijentima, rokovima, dokumentima i finansijskim podacima ne zahteva smeštanje kompletne baze na infrastrukturu NBK Code-a.

Ovakva arhitektura smanjuje broj mesta na kojima bi potpuna kancelarijska baza mogla da bude izložena i omogućava korisniku da zadrži neposrednu kontrolu nad svojim poslovnim podacima.

Licenciranje, provera nadogradnji i opcione mrežne funkcije predstavljaju odvojene tehničke procese i ne daju NBK Code-u pristup sadržaju predmeta.

2. Kriptografska zaštita baze

Podaci u mirovanju štite se primenom algoritma AES-256-GCM.

Ovaj način zaštite obezbeđuje:

- nečitljivost sadržaja bez odgovarajućeg ključa;
- proveru integriteta šifrovanih podataka;
- prepoznavanje neovlašćene izmene zaštićenog sadržaja.

Za svaku instalaciju generiše se poseban nasumični ključ za šifrovanje baze. Taj ključ se ne čuva u otvorenom obliku, već se dodatno štiti mehanizmom izvođenja i umotavanja ključa.

LexDesk podržava i kontrolisanu recovery proceduru. Recovery podatak treba čuvati odvojeno od računara na kome se nalazi baza, jer predstavlja važan deo postupka oporavka ili prenosa podataka.

Ako zaštitni mehanizam utvrdi da baza koja treba da bude zaštićena nije kriptovana, LexDesk pokreće predviđenu proceduru njene zaštite.

3. PIN zaštita i kontrola pristupa

Desktop PIN ne čuva se kao čitljiv podatak.

Za njegovu zaštitu koristi se funkcija scrypt, uz poseban nasumični salt za instalaciju. Poređenje verifikacionih vrednosti obavlja se postupkom koji umanjuje mogućnost izvlačenja informacija na osnovu vremena potrebnog za proveru.

LexDesk Companion koristi lokalnu PIN zaštitu zasnovanu na WebCrypto mehanizmu i funkciji PBKDF2-SHA-256 sa visokim brojem iteracija.

PIN zaštita je jedan sloj odbrane. Bezbednost kancelarije zavisi i od zaštite Windows naloga, fizičke kontrole računara, pravilnog čuvanja recovery podataka i ograničavanja pristupa ovlašćenim licima.

4. LexDesk Companion i dozvole uređaja

LexDesk Companion nije kopija kompletne kancelarijske baze.

Povezani uređaj dobija samo dozvoljeni operativni skup podataka i samo funkcije koje mu je vlasnik kancelarije odobrio. Dozvole za predmete, rokove, kontakte i beleške mogu se kontrolisati pojedinačno.

Svaki uređaj dobija sopstveni pristupni token generisan kriptografski bezbednim izvorom slučajnosti. Na desktop računaru ne čuva se originalna vrednost tokena, već njena kontrolna SHA-256 vrednost.

Pristup povezanog uređaja može se opozvati bez menjanja glavne kancelarijske baze.

Mrežna komunikacija štiti se TLS vezom u okviru konfigurisane privatne mreže. Sadržaj podržanih push obaveštenja dodatno se štiti standardnim Web Push mehanizmima, uključujući ECDH i AES128GCM.

5. Provera integriteta aplikacije

LexDesk pri pokretanju proverava integritet ključnih programskih artefakata.

Kontrolne SHA-256 vrednosti omogućavaju sistemu da prepozna da li je neka od zaštićenih datoteka promenjena u odnosu na odobreno izdanje.

Provera obuhvata ključne komponente LexDesk-a i integritet odabranih spoljnih izvršnih modula pre njihovog pokretanja.

Ako lokalna provera izdanja ne može da potvrdi integritet ili autentičnost zaštićenih komponenti, sistem prelazi u zaštitno stanje i sprečava nastavak rada nad podacima u neproverenom okruženju.

Ova mera smanjuje rizik da izmenjena, oštećena ili podmetnuta programska datoteka bude izvršena kao deo verifikovanog LexDesk izdanja.

6. Kriptografski potpis i bezbedne nadogradnje

Svako odobreno izdanje i nadogradnja mogu se povezati sa potpisanim manifestom izdanja.

Za potpisivanje se koristi asimetrični algoritam Ed25519:

- privatni ključ ostaje van aplikacije, instalacionog paketa i paketa nadogradnje;
- privatni ključ nalazi se u isključivom posedu odgovornog izdavaoca;
- aplikacija sadrži samo javni ključ namenjen proveru potpisa;
- javni ključ ne može da se koristi za izradu novog validnog potpisa.

Pre instaliranja nadogradnje LexDesk proverava:

- 1. identitet izdanja;
- 2. kriptografski potpis manifesta;
- 3. kontrolnu vrednost preuzetog instalacionog paketa;
- 4. podudarnost Build ID i Verification ID oznaka;
- 5. status odobrenja konkretnog izdanja.

Ako preuzeta nadogradnja nema očekivani potpis ili joj kontrolne vrednosti ne odgovaraju, instalacija se ne dozvoljava.

Neuspešna provera udaljene nadogradnje ne pretvara nepoznati paket u pouzdano izdanje. Postojeća validna instalacija i provera njenog lokalnog integriteta predstavljaju odvojen zaštitni proces.

7. Interni kriptografski žig

Interni žig LexDesk izdanja ima dve povezane uloge.

Dokaz autentičnosti i integriteta

Potpisani manifest i kontrolne vrednosti povezuju konkretno izdanje sa NBK Code lancem izdavanja. Izmena zaštićenog artefakta menja njegovu kontrolnu vrednost i prekida očekivano podudaranje.

Veza sa internom verifikacijom

Žig povezuje određenu verziju, Build ID, Verification ID, skup artefakata i status odobrenja izdanja.

Oznaka NBK CODE VERIFIED prikazuje se samo za izdanje koje je prošlo predviđeni interni postupak i dobilo status odobrenog izdanja.

Interni žig nije kvalifikovani elektronski potpis fizičkog lica i ne predstavlja sertifikaciju nezavisnog akreditovanog tela. On je tehnički mehanizam kojim NBK Code potvrđuje poreklo, integritet i interni status konkretnog softverskog izdanja.

8. Dokumentovano interno testiranje

LexDesk V2.0.0 i pripadajuće komponente prošli su interno definisan i dokumentovan postupak testiranja pre odobravanja izdanja.

Metodologija testiranja oblikovana je prema procesnom okviru standarda:

SRPS ISO/IEC/IEEE 29119-2:2021 - Softverski i sistemski inženjering - Testiranje softvera - Deo 2: Procesi testiranja.

Ovaj standard definiše procese koji se mogu koristiti za upravljanje, organizovanje i sprovođenje testiranja softvera u različitim modelima životnog ciklusa razvoja.

Za svaki sprovedeni test postoji dokument ili skup povezanih dokumenata koji, u zavisnosti od vrste provere, mogu sadržati:

- cilj i predmet testa;
- početne uslove;
- test scenario i korake;
- očekivani rezultat;
- ostvareni rezultat;

- evidentirane nepravilnosti;
- korektivne aktivnosti;
- ponovljeno testiranje;
- zaključak i status testa;
- vezu sa verzijom, Build ID i Verification ID oznakom.

Primena procesnog okvira ovog standarda ne predstavlja ISO sertifikaciju NBK Code-a niti nezavisnu potvrdu usaglašenosti. Predstavlja dokumentovan interni pristup organizovanju i sprovođenju testiranja po uzoru na priznati standard za procese testiranja softvera.

9. Uvid u dokumentaciju testiranja

Dokumentacija testiranja nije javno objavljena jer može sadržati interne test scenarije, tehničku strukturu sistema, bezbednosne pretpostavke i druge podatke čije bi potpuno javno objavljivanje moglo da umanjí bezbednost proizvoda.

NBK Code može, isključivo na obrazloženi zahtev klijenta, omogućiti kontrolisani uvid u odgovarajući deo dokumentacije testiranja za ugovorenu i isporučenu verziju LexDesk-a.

Obim i način uvida određuju se tako da se istovremeno zaštite:

- poverljivi tehnički podaci;
- privatni kriptografski ključevi;
- izvorni kod;
- podaci drugih korisnika;
- bezbednosna arhitektura čije bi potpuno otkrivanje predstavljalo rizik;
- prava intelektualne svojine NBK Code-a.

Uvid u dokumentaciju ne podrazumeva predaju privatnih ključeva, kompletnog izvornog koda niti dokumenata koji nisu povezani sa verzijom koju klijent koristi.

10. Podrška obavezama iz propisa Republike Srbije

LexDesk sadrži tehničke mere koje mogu pomoći korisniku u ispunjavanju obaveza u vezi sa bezbednošću obrade podataka o ličnosti.

Član 50 Zakona o zaštiti podataka o ličnosti predviđa tehničke, organizacione i kadrovske mere primerene riziku. Među njima se navode kriptozastita, poverljivost, integritet, raspoloživost, mogućnost oporavka i redovno testiranje delotvornosti primenjenih mera.

Za advokatske kancelarije posebno je važna obaveza čuvanja advokatske tajne. Kodeks profesionalne etike advokata ovu obavezu vezuje i za elektronske dokumente i nalaže razuman oprez prilikom elektronskog prenosa poverljivih sadržaja.

LexDesk podržava sprovođenje ovih obaveza kroz:

- lokalno čuvanje glavne baze;
- kriptografsku zaštitu podataka;
- kontrolu pristupa i dozvola;
- zaštitu prenosa;
- evidenciju i proveru integriteta;

- šifrovane rezervne kopije;
- kontrolisani oporavak;
- dokumentovano testiranje bezbednosnih mehanizama.

11. Granice tehničke zaštite

Softver ne može samostalno da garantuje potpunu zakonsku usklađenost kancelarije.

Korisnik je odgovoran za:

- zakonitost i svrhu obrade podataka;
- određivanje ovlašćenih lica;
- fizičku zaštitu računara i mobilnih uređaja;
- zaštitu Windows naloga;
- pravilno čuvanje recovery podataka;
- izradu i čuvanje rezervnih kopija;
- rokove čuvanja i brisanja podataka;
- reagovanje u slučaju bezbednosnog incidenta;
- ažurno održavanje operativnog sistema i ostalih komponenti okruženja;
- korišćenje LexDesk-a u skladu sa dokumentacijom i ugovorenom konfiguracijom.

LexDesk pruža tehničke mehanizme koji podržavaju poverljivost, integritet, raspoloživost i kontrolu pristupa. Konačna usklađenost zavisi i od organizacionih mera i stvarnog načina rada svake kancelarije.

Zaključak

LexDesk je projektovan tako da softver, baza i podaci ostanu pod kontrolom advokatske kancelarije.

NBK Code je uložio najveći mogući stručni napor da zaštita ne bude naknadno dodat sloj, već sastavni deo arhitekture proizvoda. Cilj je da se istovremeno zaštite programsko izdanje, baza i podaci korisnika, kao i da LexDesk tehničkim merama podrži ispunjavanje obaveza koje proizlaze iz zakona i profesionalnih pravila.

Zbog toga je NBK Code uveo:

- interni kriptografski žig izdanja;
- potpisani lanac izdavanja i nadogradnji;
- proveru integriteta programskih artefakata;
- dokumentovan postupak internog testiranja, oblikovan prema procesnom okviru standarda SRPS ISO/IEC/IEEE 29119-2:2021;
- vezivanje rezultata testiranja za konkretnu verziju, Build ID i Verification ID.

LexDesk je prvi proizvod NBK Code-a na kome je ovaj celovit sistem interne verifikacije i kontrole izdanja primenjen.

NBK Code je svestan da advokatska kancelarija ne čuva samo sopstvene poslovne podatke. Ona čuva podatke klijenata, stranaka i drugih lica, dokumentaciju predmeta i informacije zaštićene obavezom čuvanja advokatske tajne.

Zato LexDesk nema skriveni administratorski pristup, univerzalnu lozinku niti "zadnji ulaz" kojim bi NBK Code mogao samostalno da pristupi sadržaju kancelarije. U isporučenoj konfiguraciji NBK Code ne može bez izričitog zahteva i učešća korisnika da pregleda, kopira ili upravlja njegovom bazom i predmetima.

Softver i podaci ostaju u rukama kancelarije kojoj pripadaju.

Poruka vlasnika NBK Code-a

Zaštita nije obećanje koje se daje jednom. Ona mora da se proverava pre svakog odobrenog izdanja i svake nadogradnje.

Tek kada predviđene provere budu završene i kada izdanje ispuni uslove interne verifikacije, lično odobravam i kriptografski potpisujem njegov manifest privatnim ključem koji posedujem samo ja. Nakon potpisivanja, medij sa privatnim ključem vraća se na zaštićeno čuvanje u sef.

U LexDesk-u se nalazi samo javni deo potreban za proveru potpisa. Njime se može potvrditi da je izdanje odobreno, ali se ne može napraviti novi potpis, otključati baza niti pristupiti podacima kancelarije.

Izdavanje licencnog fajla ne otvara vezu prema NBK Code-u. Ono potvrđuje pravo korišćenja proizvoda, ali nama ne daje pristup vašim predmetima, dokumentima ili bazi.

U LexDesk-u ne postoji administratorski master-ključ niti skriveni ulaz. Niko iz NBK Code-a, uključujući i mene, ne može samostalno da uđe u vašu kancelariju i razgleda njene podatke. Ako vam ikada bude potrebna tehnička podrška koja zahteva pristup vašem okruženju, ona se može obaviti isključivo na vaš izričit zahtev, uz vaše učešće i pod vašom kontrolom.

To nije samo tehnička odluka. To je odnos prema poverenju koje nam je ukazano.

Vlasnik i odgovorno lice NBK Code-a

Reference

1. Institut za standardizaciju Srbije: SRPS ISO/IEC/IEEE 29119-2:2021, Softverski i sistemski inženjering - Testiranje softvera - Deo 2: Procesi testiranja. <https://iss.rs/en/project/show/iss%3Aproj%3A103303>
2. Zakon o zaštiti podataka o ličnosti, Službeni glasnik RS, broj 87/2018. <https://reg.pravno-informacioni-sistem.rs/api/v1ewdoc?doctype=reg®actid;=427034&uuid;=57FA21D6-0B5F-48D8-92B1-AEBBEFFC8DBC>
3. Kodeks profesionalne etike advokata, Službeni glasnik RS, broj 27/2012. <https://aks.org.rs/aks/wp-content/uploads/2015/10/Kodeks-profesionalne-etike-2012.pdf-SLGL-27-2012.pdf>