

Postopek elektronskega poslovanja in vlaganja zahtevkov z uporabo dvofaktorske avtentikacije (2FA)

Družba za upravljanje, v skladu z točko 10.2.1 Prospekta z vključenimi pravili upravljanja Krovnega sklada Infond, predhodno pregledanim in identificiranim vlagateljem omogoča vlaganje in podpisovanje zahtevkov (pristopna izjava, zahteva za izplačilo, zahteva za prehod, sklenitev direktne obremenitve, sprememba zneska direktne obremenitve, ukinitvev ali preklic direktne obremenitve) s pomočjo dvofaktorske avtentikacije (2FA).

1 Pojasnilo pojmov

Dvofaktorska avtentikacija (v nadaljevanju 2FA) je način oziroma metoda, sestavljena iz dveh avtentikacijskih faktorjev z namenom povečati varnost pri istovetnosti in avtentikaciji vlagatelja, da se zagotovi nivo močne overitve.

Močno overjanje je postopek, ki temelji na uporabi dveh ali več faktorjev:

- S** nekaj, kar ve samo uporabnik (v primeru spodaj navedenega postopka je to uporabniško ime in geslo),
- S** nekaj, kar je v izključni lasti uporabnika (v primeru spodaj navedenega postopka je to mobilni telefon, na katerega posredujemo enkratno geslo),
- S** nekaj, kar uporabnik je.

Avtentikacija s SMS žetonom oziroma enkratno kodo je mehanizem, prek katerega se ustvari geslo za enkratno uporabo, ki se pošlje na potrjeno mobilno številko uporabnika.

2 Pogoji za uporabo 2FA

Pogoji za uporabo 2FA

- S** vlagatelj je predhodno pregledan in identificiran,
- S** vlagatelj družbi poleg potrebnih podatkov za identifikacijo posreduje tudi številko mobilnega telefona,
- S** vlagatelj izvede prvo registracijo, kot je to zapisano v postopku uporabe 2FA.

3 Postopek uporabe 2FA

Registracija

Osnovo za prvo registracijo v aplikacijo predstavlja registracijski postopek za portal Savanet, ki zajema vse podatke, potrebne za prijavo z 2FA. Gre za zajem e-poštnega naslova, mobilne telefonske številke in gesla. Elektronska pošta in mobilna številka se obe preverita, da ima registrirajoči se uporabnik res lastništvo oz. dostop do njiju (s potrditveno povezavo na e-mail oz. SMS kodo), geslo pa z dvakratnim vnosom uporabnika, vse skupaj pa dodatno verificira s postopkov verifikacije lastnika. Ko je lastništvo teh (kontaktnih) podatkov potrjeno, se lahko prijavni podatki uporabijo za prijavo v sistem in izvajanje aktivnosti.

Omogočeni so tudi postopki menjave e-poštnega naslova, mobilne telefonske številke in gesla, prav tako pa tudi reševanje uporabnika iz situacije, če se geslo pozabi. S tem so zagotovljeni pogoji uporabnosti za izvedbo 2FA. Na ta način je zagotovljena večja varnost prijave, ki pa zahteva en dodatni korak pri prijavi (uporaba drugega faktorja). Pogoj za vklop je verificirana mobilna telefonska številka.

Potrjevanje zahtevkov

Po uspešni registraciji lahko uporabnik izvaja različne akcije. Za izvedbo in potrjevanje zahtevkov (npr. pristop k skladu, oddaja zahtevka za izplačilo...) se prav tako smiselno zahteva uporabo drugega faktorja in takšno aktivnost varnostno tudi ustrezno beleži.

Za izvedbo oz. potrjevanje zahtevkov (npr. pristop k skladu, oddaja zahtevka za izplačilo, sklenitev direktne obremenitve...) sistem od uporabnika prav tako zahteva uporabo drugega faktorja (uporaba mobilne telefonske številke, na katero uporabnik dobi časovno omejeno enkratno kodo, ki jo mora vnesti za potrditev akcije) in takšno aktivnost varnostno ustrezno zabeleži. Potrjene podatke in podatke o postopku potrjevanja sistem kot celoto podpiše z digitalnim potrdilom (strežniški elektronski podpis), s čimer se zagotavlja tudi nespremenljivost vnesenih in potrjenih podatkov.