Projekt e-Građani

Pravilnik
o postupcima izdavanja
korisničkog imena i lozinke ePass za e-građane
(Password Practice Statement - PPS)

Verzija 1.2

Zagreb, travanj 2014.

Naslov:

Pravilnik o postupcima izdavanja korisničkog imena i lozinke ePass za e-građane (Password Practice Statement - PPS)

Opis:

Dokument sadrži odredbe o postupcima izdavanja korisničkog imena i lozinke ePass u sustavu e-Građani

Ključne riječi:

Projekt e-Građani, ePass, pravilnik, postupak, korisničko ime, lozinka

Jezik:

Hrvatski

Stvaratelji:

Financijska agencija
Ministarstvo uprave, Uprava za e-Hrvatsku

Izdavač:

Ministarstvo uprave, Uprava za e-Hrvatsku

Mjesto i datum stupanja na snagu:

Zagreb, 10. travanj 2014.

Izvor:

Financijska agencija

SADRŽAJ

DEFINICIJE

Korisnik – fizička osoba kojoj se izdaje korisničko ime/lozinka

KRATICE I POJMOVI

PPS – Password Practice Statement – Pravilnik o postupcima izdavanja korisničkog imena/lozinke

NIAS – Nacionalni identifikacijski i autentifikacijski sustav

e-Građani - projekt koji fizičkim osobama omogućava pristup javnim informacijama i informacijama o javnim uslugama na jednom mjestu, siguran pristup osobnim podacima i elektroničku komunikaciju građana i javnog sektora. Projekt e-Građani je koncipiran kroz tri sastavnice i to: sustav Središnjeg državnog portala, Nacionalni identifikacijski i autentifikacijski sustav (NIAS) i sustav Osobnog korisničkog pretinca. Projekt je pokrenut Odlukom Vlade RH 25.04.2013 NN 52/13.

1 UVOD

Fina kao izdavatelj vjerodajnica u ime Republike Hrvatske izdaje građanima Republike Hrvatske korisničko ime/lozinku u okviru e-Građana naziva ePASS koji se koristi u svrhu pristupa određenim javnim servisima i uslugama (projekt e-Građani) putem NIAS-a.
Ovaj Pravilnik (dalje u tekstu: PPS) opisuje opća pravila i postupke izdavanja korisničkih imena i lozinki ePASS te određuje obveze i prava korisnika i Fine kao izdavatelja vjerodajnice.

Također, PPS obuhvaća i određuje određene sigurnosne procedure i pravila izdavanja i korištenja ovih vjerodajnica.

Svi sudionici se obvezuju poštivati odredbe PPS-a.

2 SUDIONICI I OBVEZE

2.1 Sudionici

Sudionici u ovom sustavu su:

- Fina kao izdavatelj korisničkog imena/lozinke ePASS;
- korisnici kojima se izdaje korisničko ime/ lozinka ePASS;
- servisi odnosno usluge koje koriste korisničko ime/lozinku ePASS kao sredstvo autentifikacije i autorizacije korisnika.

2.2 Obveze i odgovornosti Fine

Ovlaštene osobe Fine dužne su, tijekom postupka registracije korisnika, ustanoviti točnost i cjelovitost podataka na osnovu kojih se izdaje korisničko ime/lozinka ePASS kroz provjeru identifikacijskog dokumenta, fizičke identifikacije i upita na mjerodavne registre (OIB sustav).

Fina se obvezuje voditi evidenciju o svim dodijeljenim korisničkim imenima/lozinkama ePASS.

Fina je dužna osigurati način preuzimanja i kreiranja korisničkog imena i lozinke u takvoj mjeri da zadovoljava uvjete sigurnosne razine 2 (Kriteriji za određivanje razine osiguranja kvalitete autentifikacije[1]).

Fina je dužna poduzeti mjere unutar svojih mogućnosti i nadležnosti da neovlaštenim osobama ili napadačima spriječi pristup osobnim podacima korisnika, odnosno dozvoli pristup osobnim podacima korisnika samo ovlaštenim osobama.

Fina je kao izdavatelj korisničkog imena/lozinke ePASS dužna poštovati propise koji reguliraju zaštitu osobnih podataka tijekom cijelog životnog ciklusa osobnih podataka.

Fina je dužna izraditi i objaviti PPS dokument na način da je isti lako dostupan svim korisnicima i zainteresiranim stranama.

[1] Dokument objavljen na stranicama Ministarstva uprave RH: http://www.uprava.hr/UserDocsImages/eHrvatska/eGradjani/NIAS%20-%20Kriteriji%20za%20odredjivanje%20razine%20osiguranja%20kvalitete%20autentifikacije%20u%20sustavu%20NIAS%20(Ver.%201.2).pdf

2.3 Obveze i odgovornosti Korisnika

Korisnici su odgovorni ispunjavati sve odredbe ovog PPS-a, uključujući, ali ne i ograničavajući na slijedeće specifične odgovornosti:

Korisnici moraju lozinku čuvati tajnom.

Korisnici moraju zadržati jedinstvenu kontrolu nad lozinkom. Korisnici ne smiju dijeliti ili davati svoju lozinku drugim osobama ili subjektima.

Korisnici su odgovorni odabrati snažne lozinke koje je teško pogoditi. Lozinka mora zadovoljavati sljedeće kriterije:

- sadržava barem jedno veliko slovo;
- sadržava barem jedno malo slovo;
- sadržava barem jednu znamenku;
- sadržava najmanje 8 znakova;
- ne smije sadržavati znakove č,ć,š,đ,ž,Č,Ć,Š,Đ,Ž:

Savjetuje se:

- korištenje kombinacije malih i velikih slova (npr. d, D), brojeva (npr. 3, 6) i specijalnih znakova (npr. !, &);
- izbjegavanje ponavljajućih ili na tipkovnici slijednih znakova.

Korisnici moraju obavijestiti Finu u slučaju da sumnjaju da im je lozinka otkrivena ili poznata bilo kojoj drugoj osobi ili subjektu ili je na bilo koji drugi način ugrožena.

Korisnici moraju obavijestiti Finu ukoliko su zaboravili vlastitu lozinku i tražiti izdavanje nove ili zatvaranje računa.

Korisnici moraju obavijestiti Finu u slučajevima kada korištenjem vlastite lozinke nisu u stanju spojiti se ni na jedan servis.

Korisnici moraju koristiti lozinku u za to predviđene svrhe.

2.4 Obveze i odgovornosti servisa i usluga

Kako se korisničko ime/lozinka ePASS izdaje kao elektronički identitet u svrhu pristupa servisima i uslugama kroz projekt e-Građani kroz sustav NIAS, servisi i usluge u kojima će se koristiti ovaj elektronički identitet su NIAS i servisi i usluge projekta e-Građani.

Obveza NIAS-a, servisa i usluga je omogućiti korištenje korisničkog imena/lozinke ePASS u skladu sa procijenjenom razinom sigurnosti ovog elektroničkog identiteta.

3 PROCES IZDAVANJA ELEKTRONIČKOG IDENTITETA KORISNIČKO IME/LOZINKA EPASS

Proces izdavanja korisničkog imena/lozinke je podijeljen na niz smislenih i međusobno povezanih cjelina.

3.1 Registracija korisnika

Registracija korisnika se vrši u poslovnicama Fine. Korisnik ugovara dobivanje korisničkog imena/lozinke ePASS tako da cjelovito i točno popuni Pristupnicu za dodjeljivanje ePASS korisničkog imena/lozinke.

Prilikom predavanja zahtjeva, ovlaštena osoba Fine identificira korisnika provjerom u važeći službenog identifikacijskog dokumenta, fizičkom identifikacijom korisnika te usporedbom dobivenih podataka s podacima iz OIB sustava. Osobe koje mogu pristupiti postupku registracije trebaju imati navršenih 15 godina starosti i OIB. Osobe koje nisu rezidenti Republike Hrvatske mogu pristupiti postupku registracije uz prethodno ispunjene uvjete.

Po provjeri podataka, djelatnik popunjava i dodatni skup podataka koji nisu dohvatljivi iz OIB sustava. Ovi podaci uključuju:

- adresu elektroničke pošte korisnika;
- kontakt brojeve telefonskog/mobilnog uređaja korisnika

3.2 Izdavanje aktivacijskih podataka

Nakon pozitivne identifikacije i registracije korisnika, ovlaštena osoba Fine šalje upit sustavu koji generira aktivacijske podatke za korisnika kojim će korisnik moći ostvariti siguran i individualiziran pristup internetskoj aplikaciji gdje će odabrati svoje korisničko ime i lozinku.

Aktivacijski podaci su:

- Aktivacijski link koji se šalje na adresu korisnikove elektroničke pošte;
- Aktivacijski kod za aktiviranje korisničkog računa.

Aktivacijski kod se predaje korisniku na ruke i važi 14 dana od dana izdavanja.
Korisnik potpisuje da je osobno preuzeo aktivacijski kod.
Aktivacijski kod se može pokušati upotrijebiti do 5 puta, za slučajeve prekida sesije ili nepotpunog odabira korisničkog imena i lozinke. Po ispravnom i dovršenom postupku odabira korisničkog imena i lozinke, aktivacijski kod postaje neaktivan.

3.3 Proces odabira korisničkog imena/lozinke ePASS i kreiranje korisničkog profila

Korisnik prvi put pristupa svom računu putem aktivacijskog linka iz elektroničke poruke koji ga upućuje na upis aktivacijskog koda koji je dobio u poslovnici Fine.
Točnim upisom aktivacijskog koda omogućuje mu se odabir korisničkog imena i lozinke.
Korisničko ime nije tajan podatak, nije osjetljiv na velika i mala slova i korisnik ga proizvoljno odabire.

Nakon potvrde da je odabrano korisničko ime dostupno, korisnik odabire lozinku i potvrđuje je ponovnim upisom. Preporuka je da se lozinka odabire tako da se što više oteža njezino pogađanje, po pravilima iz točke 2.3. ovog PPS-a.
Po prihvaćanju lozinke kreiran je korisnički račun odnosno korisničko ime/lozinka.
Korisnička lozinka se nikada ne sprema u Fininin datotečni sustav u čitljivom tekstu, već se obrađuje SHA1 + salt kriptografskom metodom i kao takva sprema u Finin datotečni sustav.

3.4 Korištenje i upravljanje korisničkim računom

Kad se prijavi, korisnik je u mogućnosti mijenjati određene podatke na svom profilu:

- adresu elektroničke pošte;
- broj kućnog telefona;
- broj mobilnog telefona;
- lozinku.

Korisnik mora odgovoriti na kontrolno pitanje po vlastitom izboru, a odgovor će biti poznat samo korisniku. U slučaju da je korisnik zaboravio lozinku, ima mogućnost kreirati novu, ali mora točno odgovoriti na postavljeno pitanje.

Ukoliko korisnik ne odgovori točno na kontrolno pitanje u 5 pokušaja, korisnički račun se zaključava.
Korisnički račun se može otključati samo pomoću novog aktivacijskog koda i aktivacijskog linka koje korisnik može dobiti isključivo u poslovnici Fine.

Zatvaranje korisničkog računa je moguće kroz korisnički portal na internetu ili u poslovnici Fine. Zatvaranje je trajno i za ponovno otvaranje korisnik mora doći u poslovnicu Fine.

4 NAČIN PRIHVATA VJERODAJNICA KOJE NISU IZDANE U FINI

Drugi izdavatelji vjerodajnice mogu ustupiti podatke o svojim korisnicima Fini kako bi se njihove postojeće vjerodajnice iskoristile za dobivanje korisničkog imena/lozinke ePASS. Time prestaje vrijediti vjerodajnica drugog izdavatelja vjerodajnice, a korisnik je oslobođen od osobnog dolaska u poslovnicu Fine za potrebe registracije. Drugi izdavatelj vjerodajnice prije ustupanja podataka treba proći proceduru audita za ocjenu razine osiguranja kvalitete autentifikacije za Nacionalni identifikacijski i autentifikacijski sustav (NIAS).

Promjena korisničkog imena/lozinke drugog izdavatelja u korisničko ime/lozinku ePASS se obavlja na web stranicama ePASS-a. Korisnik im može pristupiti direktno ili preko NIAS-a u trenutku odabira vjerodajnice za autentifikaciju na e-usluge. Ova promjena se obavlja jednokratno. U tom procesu se obavlja i provjera ispravnosti podataka i usporedba s podacima dostavljenim od strane drugog izdavatelja vjerodajnice.
Ukoliko je potvrđena ispravnost korisničkog imena i lozinke drugog izdavatelja vjerodajnice, upisuju se novi podaci relevantni za izdavanje korisničkog imena/lozinke ePASS (navedeno u 3.1 i 3.4).

Korisnici, čiji podaci ne udovoljavaju pravilima sustava ePASS za izdavanje korisničkog imena/lozinke, prilikom preuzimanja podataka od drugog izdavatelja vjerodajnice, će o tome biti

obaviješteni korisničkom porukom u trenutku pokušaja promjene, te će biti upućeni da otvaranje korisničkog računa u ePASS sustavu obave na registracijskom mjestu.

Pogrešan unos korisničkog imena i lozinke drugog izdavatelja moguće je ponoviti u 5 pokušaja, nakon čega će korisnik dobiti poruku da proces registracije obavi osobnim dolaskom na registracijskom mjestu.

Nakon uspješne potvrde ispravnosti, korisnik nastavlja proces kreiranja i korištenja svog korisničkog imena i lozinke u sustavu ePASS prema proceduri opisanoj u poglavljima 3.1, 3.2, 3.3 i 3.4.