Smernice za izbiro zahtevane ravni zanesljivosti sredstva elektronske identifikacije za dostop do elektronskih storitev v javnem sektorju

Smernice so pripravljene in objavljene na portalu nacionalnega interoperabilnostnega okvira (v nadaljnjem besedilu: portal NIO) v skladu s 50. členom Uredbe o določitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis (Uradni list RS, št. 29/22) v povezavi s 15. členom Zakona o elektronski identifikaciji in storitvah zaupanja (Uradni list RS, št. 121/21, 189/21 – ZDU-1M in 18/23 – ZDU-1O, v nadaljnjem besedilu: ZEISZ).

ZEISZ namreč ureja tudi osebno elektronsko identiteto, ki jo dodeli Republika Slovenija, in sredstva elektronske identifikacije, s katerimi se dokazuje ta elektronska identiteta v skladu z zahtevami iz Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES, v nadaljnjem besedilu: uredba eIDAS).

1) Uvod

Sredstva elektronske identifikacije so bolj ali manj odporna na zlorabe in spreminjanje identitet, zato je stopnja zanesljivosti ugotovljene elektronske identitete uporabnika storitve v veliki meri odvisna od vrste uporabljenega sredstva elektronske identifikacije. Posledično imajo morebitne zlorabe in nepravilnosti pri ugotavljanju in preverjanju identitete različne posledice za različne storitve.

Organ javnega sektorja, ki ponuja elektronsko storitev, za dostop do katere je potrebna elektronska identifikacija in avtentikacija uporabnika (v nadaljevanju ponudnik storitev) in za katero mora določiti raven zanesljivosti elektronske identifikacije, mora določiti minimalno raven, ki je zanj še sprejemljiva. Pri tem je priporočljivo, da izbere takšno raven zanesljivosti, ki najbolj ustreza njegovim varnostnim zahtevam in morebitnim tveganjem. Določitev nižje ravni ni dopustna z varnostnega vidika, višja raven pa lahko naloži uporabnikom in ponudniku storitev izpolnjevanje dodatnih zahtev in z njimi povezane stroške.

1.1) Namen in cilji

Namen tega dokumenta je pomagati ponudnikom storitev izbrati najustreznejšo zahtevano raven zanesljivosti sredstva elektronske identifikacije, ki se uporablja za njihovo storitev.

2) Predstavitev ravni zanesljivosti

Raven zanesljivosti označuje stopnjo zanesljivosti, da je oseba, ki izkazuje elektronsko identiteto, dejansko oseba, ki ji je bila ta elektronska identiteta dodeljena. ZEISZ določa tri ravni zanesljivosti:

- Nizka raven – zagotavlja **omejeno** stopnjo zanesljivosti v izkazano identiteto osebe, namen uporabljenih postopkov je **zmanjšati** nevarnost zlorabe ali spreminjanja identitete;

- Srednja raven – zagotavlja **srednjo** stopnjo zanesljivosti v izkazano identiteto osebe, namen uporabljenih postopkov je **znatno zmanjšati** nevarnost zlorabe ali spreminjanja identitete;

- Visoka raven – zagotavlja **višjo** stopnjo zanesljivosti v izkazano identiteto osebe, kot je izkazana s sredstvom elektronske identifikacije srednje ravni zanesljivosti, namen uporabljenih postopkov je **preprečiti** nevarnost zlorabe ali spreminjanja identitete.

Sredstva elektronske identifikacije, elektronska identifikacija in zahteve za ponudnike storitev se na posameznih ravneh razlikujejo v več vidikih.

Raven zanesljivosti je odvisna od načina dokazovanja in preverjanja identitete pravne ali fizične osebe ob registraciji (na primer z identifikacijskim dokumentom brez slike ali s sliko), vrste povezave med sredstvi elektronske identifikacije fizičnih in pravnih oseb, načina izdajanja, dostave in aktiviranja sredstev za elektronsko identifikacijo, načina upravljanja s sredstvi, odpornosti na varnostne grožnje pri avtentikaciji ter postopkov upravljanja izdajateljev sredstev.

Na primer, če pri nizki ravni zadostuje, da sredstvo elektronske identifikacije uporablja en dejavnik avtentikacije (npr. geslo ali zasebni kriptografski ključ ali prstni odtis), morata biti pri srednji ravni dejavnika vsaj dva (dvofaktorska avtentikacija, npr. poleg uporabniškega imena in gesla še žeton za enkratno prijavo). Pri visoki ravni je dodatna zahteva na primer še ta, da v sredstvo (npr. pametno kartico) ni mogoče fizično poseči in iz nje prebrati kriptografskega ključa.

Primeri sredstev elektronske identifikacije za posamezne ravni zanesljivosti so:

- Nizka raven (kasneje tudi: *N*) – sredstvo nizke ravni na osebni izkaznici, sredstva nizke ravni zanesljivosti po uredbi eIDAS;

- Srednja raven (kasneje tudi: *S*) – virtualno sredstvo srednje ravni, sredstva srednje ravni zanesljivosti po uredbi eIDAS;

- Visoka raven (kasneje tudi: *V*) – sredstvo visoke ravni na osebni izkaznici, sredstva visoke ravni zanesljivosti po uredbi eIDAS.

3) Ocena tveganja

Za namene določitve ravni zanesljivosti sredstva elektronske identifikacije za dostop do elektronskih storitev v javnem sektorju mora ponudnik storitev najprej oceniti stopnjo tveganja, če identiteta subjekta, ki uporablja njegovo storitev, ni enaka identiteti, ki se izkazuje, oziroma če oseba, ki izkazuje določeno identiteto, ni oseba, ki ji je bila ta identiteta dejansko dodeljena. Ker se ocena lahko razlikuje pri različnih načinih uporabe storitve, je treba oceno opraviti za vsak način uporabe posebej. (Primera različnih načinov uporabe storitve sta na primer pregled oddanih vlog in oddaja nove vloge.)

Stopnjo tveganja ponudnik oceni s pomočjo več kriterijev. Kriteriji so povezani s posledicami napačnega ugotavljanja identitete, zlorabe ali spremembe identitete, na primer s pravnimi posledicami, z zmanjšanjem ali izgubo ugleda ponudnika storitev, povzročeno ekonomsko škodo in odgovornostjo, vplivom na aktivnosti ponudnika in javni interes ter nepooblaščenim razkritjem osebnih podatkov. Raven zanesljivosti se lahko določi tudi z zakonodajo.

Stopnja tveganja je odvisna od velikosti povzročene škode, če pride do nepravilnosti, ocenjujemo pa jo z vrednostmi nizka, srednja in visoka. Višja stopnja tveganja zahteva določitev višje ravni zanesljivosti

uporabljenih sredstev elektronske identifikacije. Verjetnost dogodka, ki prav tako vpliva na stopnjo tveganja, sama po sebi ni kvantitativno ovrednotena, je pa posredno upoštevana skozi kriterije.

Določanje verjetnosti dogodkov in velikosti škode je pri ocenjevanju tveganj pogosto zapleteno in dolgotrajno. Namen tega dokumenta je poenostaviti, poenotiti in olajšati ocenjevanje tveganj s pomočjo vnaprej določenih vrednosti posameznih kriterijev za vsako od treh ravni zanesljivosti in stremeti k situaciji, da bi različni ponudniki storitev v praksi v podobnih primerih prišli do enakih rezultatov. Kljub opredeljenim smernicam je ponudnik storitev še vedno sam odgovoren za izbiro ustrezne ravni.

Posamezni kriteriji in nabor njihovih vrednosti so podrobneje predstavljeni v nadaljevanju, ravni zanesljivosti pa v naslednjem poglavju.

Uporaba visoke ravni zanesljivosti se predvideva le v redkih primerih, ki zahtevajo uveljavljanje zelo visokih varnostnih zahtev.

3.1) Pravne posledice

Kadar ima storitev pravno podlago oziroma je bila njena vzpostavitev zahtevana s strani zakonodaje, imajo lahko nepravilnosti pri ugotavljanju elektronske identitete ali njena zloraba pravne posledice za ponudnika in uporabnika storitve.

Vrednosti kriterija:

- N: Storitev ima posredne pravne posledice
- S: Storitev ima neposredne pravne posledice, na katere lahko vpliva posameznik (na primer: gre za storitev, ki predvideva pritožbo posameznika v primeru nepravilnosti)
- V: Storitev ima neposredne pravne posledice, na katere posameznik ne more vplivati

3.2) Pravne zahteve

Zahteve za uporabo posameznega sredstva elektronske identifikacije so lahko neposredno ali posredno določene že s samo zakonodajo, na primer s področno zakonodajo, ki bi izrecno zahtevala uporabo sredstev elektronske identifikacije visoke ravni zanesljivosti.

Vrednosti kriterija:

- N: Zakonodaja zahteva uporabo sredstev elektronske identifikacije najmanj nizke ravni zanesljivosti
- S: Zakonodaja zahteva uporabo sredstev elektronske identifikacije najmanj srednje ravni zanesljivosti
- V: Zakonodaja zahteva uporabo sredstev elektronske identifikacije visoke ravni zanesljivosti

3.3) Osebni podatki

Zbiranje, shranjevanje in obdelava osebnih podatkov zahtevajo ustrezne zaščitne ukrepe, med katere sodi tudi avtentikacija uporabnikov, ki posredujejo in spreminjajo svoje podatke ali dostopajo do svojih podatkov ali podatkov drugih oseb. Z uporabo ustreznih sredstev elektronske identifikacije lahko zmanjšamo tveganje, da bi dostop do osebnih podatkov imele nepooblaščene osebe ali da posredovani/spremenjeni podatki ne bi bili pravi.

Nabor vrednosti pri obeh kriterijih (posredovanje lastnih osebnih podatkov, prikaz osebnih podatkov) je enak.

Vrednosti kriterijev:

- N: Osebni podatki, ki niso opredeljeni kot posebna vrsta osebnih podatkov in se ne obdelujejo v zvezi s kazenskimi obsodbami in prekrški
- S: Osebni podatki, ki so opredeljeni kot posebna vrsta osebnih podatkov ali se obdelujejo v zvezi s kazenskimi obsodbami ter prekrški, ali finančni podatki subjekta
- V: Biometrični podatki za namene edinstvene identifikacije posameznika ali zbrani podatki preiskovalnih uradov

3.4) Registri identifikacijskih podatkov

Kriterij obravnava shranjevanje in spreminjanje identifikacijskih podatkov (atributov) v osnovnih podatkovnih registrih, na primer Centralnem registru prebivalstva.

Vrednosti kriterija:

- N: Brez spreminjanja in kreiranja
- S: Spreminjanje podatkov v osnovnih registrih
- V: Kreiranje podatkov v osnovnih registrih

3.5) Ekonomska škoda

Ekonomska škoda, kot posledica zlorabe identitete ali nepravilnosti pri elektronski identifikaciji, je lahko neposredna ali posredna, zadeva pa uporabnika in ponudnika storitve. Neposredna škoda se na primer izraža kot finančna škoda zaradi kraje identitete pri uporabniku ali kazni zaradi nespoštovanja zakonskih in pogodbenih obveznostih, posredna pa skozi zmanjšanje ugleda.

Vrednosti kriterija:

- N: Omejena ekonomska škoda za uporabnika
- S: Večja ekonomska škoda za uporabnika in omejena poslovna škoda
- V: Znatna ekonomska in poslovna škoda

3.6) Javni interes

Posledica zlorab in nepravilnosti pri ugotavljanju in potrjevanju elektronske identitete so zadeve in problemi, ki imajo vpliv na aktivnosti ponudnika storitev, in zadeve in problemi javnega interesa, na primer politični ali socialni.

Vrednosti kriterija:

- N: Omejen vpliv na aktivnosti ponudnika storitev; problemi, ki jih je mogoče razrešiti znotraj ene organizacije
- S: Večji vpliv na aktivnosti ponudnika storitev; problemi, ki zahtevajo usklajeno delovanje več organizacij
- V: Zelo velik vpliv na aktivnosti ponudnika storitev; izredne razmere v družbi, ki zahtevajo takojšnje ukrepanje

3.7) Osebna varnost

Zlorabe in nepravilnosti lahko posredno ali neposredno vplivajo na osebno varnost in zdravje uporabnika.

Vrednosti kriterija:

- N: Ni posledic za osebno varnost in zdravje
- S: Minimalne posledice, ki ne zahtevajo medicinske pomoči
- V: Poškodbe, ki zahtevajo medicinsko pomoč

4) Izbira zahtevane ravni zanesljivosti

Ravni zanesljivosti so določene z vrednostmi kriterijev iz prejšnjega poglavja. Ponudnik storitev najprej za vsak kriterij oceni, kakšne so morebitne posledice, če bi pri uporabi njegove storitve prišlo do zlorabe elektronske identitete ali nepravilnosti pri ugotavljanju in potrjevanju identitete.

S pomočjo dobljenih vrednosti posameznih kriterijev določi zahtevano raven zanesljivosti na naslednji način:

- zahtevana raven zanesljivosti je visoka, če ima katerikoli izmed kriterijev vrednost V,
- zahtevana raven zanesljivosti je srednja, če ima katerikoli izmed kriterijev vrednost S, nobeden od njih pa nima vrednosti V,
- zahtevana raven zanesljivosti je nizka, če imajo vsi kriteriji vrednost N.

Primeri:

- če v primeru zlorab ali nepravilnosti nastanejo neposredne pravne posledice, je lahko izbrana raven le srednja ali visoka;
- če lahko nastane le omejena ekonomska škoda, so lahko izbrane vse tri ravni (nizka, srednja ali visoka);
- če storitev omogoča kreiranje podatkov v osnovnih registrih, je lahko izbrana raven le visoka, ne glede na vrednosti ostalih kriterijev.

5) Upoštevanje zahtevane ravni zanesljivosti

Če ponudnik storitev ugotovi, da je za uporabo storitve zahtevana srednja ali visoka raven zanesljivosti, je v skladu z določili ZEISZ in uredbe eIDAS dolžan priznati tudi vsa sredstva elektronske identifikacije, ki so bodisi po uredbi eIDAS priglašena s strani držav članic EU bodisi na podlagi ZEISZ izdana s strani države in so ravni zanesljivosti, ki je enaka ali višja od zahtevane ravni zanesljivosti.

Če ponudnik storitev ugotovi, da za uporabo storitve zadošča nizka raven zanesljivosti ali da storitev niti ne izpolnjuje zahtev zanjo, določil ZEISZ in uredbe eIDAS o priznavanju sredstev elektronske identifikacije ni dolžan upoštevati. Kljub temu pa se lahko odloči, da bo dostop do svoje storitve omogočal tudi na podlagi uporabe sredstev elektronske identifikacije, kot jih določata ZEISZ in uredba eIDAS.