EVROPSKA UNIJA
EVROPSKI
SOCIALNI SKLAD
NALOŽBA V VAŠO PRIHODNOST

Smernice za izbiro ravni zanesljivosti SI-CAS

1) Uvod

Sredstva elektronske identifikacije so bolj ali manj odporna na zlorabe in spreminjanje identitet, zato je stopnja zanesljivosti v ugotovljeno e-identiteto uporabnika storitve v veliki meri odvisna od vrste uporabljene elektronske identifikacije. Prav tako imajo morebitne zlorabe in nepravilnosti pri ugotavljanju in preverjanju identitet različno resne posledice za različne storitve.

Ponudnik storitev, ki preverjanje in potrjevanje e-identitete prenese na SI-CAS, mora določiti minimalno raven zanesljivosti sredstev elektronske identifikacije, ki je zanj še sprejemljiva. Priporočljivo je, da izbere takšno raven zanesljivosti, ki najbolj ustreza njegovim varnostnim zahtevam in morebitnim tveganjem. Nižja raven ni dopustna z varnostnega vidika, višja raven pa lahko naloži uporabnikom in ponudniku storitev dodatne zahteve in z njimi povezane stroške.

1.1) Namen in cilji

Namen tega dokumenta je pomagati ponudnikom storitev izbrati najustreznejšo zahtevano raven zanesljivosti za njihovo storitev.

2) Predstavitev ravni zanesljivosti SI-CAS

Raven zanesljivosti označuje stopnjo zanesljivosti, da je oseba, ki izkazuje določeno identiteto, dejansko oseba, ki ji je bila ta identiteta dodeljena. SI-CAS določa štiri ravni zanesljivosti:

- Zelo nizka raven – zagotavlja **minimalno** stopnjo zanesljivosti v izkazano in nepreverjeno identiteto osebe, namen uporabljenih postopkov je v **manjši meri zmanjšati** nevarnost zlorabe ali spreminjanja identitete;

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

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

- Visoka raven - zagotavlja **višjo** stopnjo zanesljivosti v izkazano ali zagotavljano identiteto osebe kot sredstva 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 zanesljivosti 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, načina upravljanja in organizacije ponudnikov storitev in opravljenega tehničnega nadzora izdajateljev sredstev.

Na primer, če pri nižjih ravneh 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. žeton za enkratno prijavo, ki ga je treba aktivirati z geslom). Pri visoki ravni je dodatna zahteva 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 SI-CAS so:

- Zelo nizka raven (raven 1) – Facebook račun, geslo;
- Nizka raven (raven 2) - sredstva nizke ravni zanesljivosti po uredbi eIDAS;
- Srednja raven (raven 3) – kvalificirano potrdilo, sredstva srednje ravni zanesljivosti po uredbi eIDAS;
- Visoka raven (raven 4) – kvalificirano potrdilo na pametni kartici, sredstva visoke ravni zanesljivosti po uredbi eIDAS.

3) Ocena tveganja

Ponudnik storitev mora najprej oceniti stopnjo tveganja, da identiteta subjekta, ki uporablja njegovo storitev, ni enaka identiteti, ki se izkazuje, oziroma da oseba, ki izkazuje določeno identiteto, ni oseba, ki ji je bila ta identiteta dejansko dodeljena. Ocena se lahko razlikuje za različne primere uporabe storitve (profile), zato je treba oceno opraviti za vsak profil posebej. Primera načina uporabe sta pregled oddanih vlog in oddaja nove vloge.

Stopnjo tveganja se ocenjuje 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 je lahko vnaprej posredno določena tudi z zakonodajo.

Stopnja tveganja je odvisna od velikosti povzročene škode v primeru, da pride do nepravilnosti, ocenjujemo pa jo z zelo nizka, nizka, srednja in visoka. Višja stopnja tveganja zahteva višjo raven zanesljivosti za uporabljena sredstva elektronske identifikacije. Verjetnost dogodka, ki prav tako vpliva na stopnjo tveganja, v našem primeru ni kvantitativno ovrednotena, je pa posredno upoštevana skozi kriterije.

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

Kriteriji in morebitne vrednosti so podrobneje predstavljeni v nadaljevanju, ravni zanesljivosti pa v naslednjem poglavju.

Uporaba visoke ravni zanesljivosti se predvideva le v redkih primerih z zelo visokimi varnostnimi zahtevami.

3.1) Pravne posledice

Kadar ima storitev pravno podlago oziroma je bila njena vzpostavitev zahtevana s strani zakonodaje, imajo lahko nepravilnosti in zlorabe e-identitete pravne posledice za ponudnika in uporabnika storitve.

Vrednosti kriterija:
Storitev lahko nima pravnih posledic ali pa so posledice posredne ali neposredne.

3.2) Pravne zahteve

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

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 ustreznimi sredstvi 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:
- ZN: Javno dostopni osebni podatki, ki ne predstavljajo tveganja za posameznika
- N: Osebni podatki, ki niso opredeljeni kot občutljivi osebni podatki (opredeljeni v 6. členu Zakona o varstvu osebnih podatkov)
- S: Občutljivi osebni podatki ali finančni podatki subjekta
- V: Občutljivi osebni podatki o zdravstvenem stanju pacientov in biometrične značilnosti, 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:

- ZN: Brez ekonomske škode
- 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 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:

- ZN: Brez posledic
- N: Minimalne posledice, ki ne zahtevajo medicinske pomoči
- S: Manjše poškodbe, ki zahtevajo medicinsko pomoč
- V: Resne poškodbe, lahko tudi smrt

4) Izbira ustrezne ravni zanesljivosti SI-CAS

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 ustrezno raven zanesljivosti na podlagi Tabele 1. Izbrana raven zanesljivosti je tista najnižja raven, pri kateri ponudnikove ocene vrednosti kriterijev ne presegajo minimalnih vrednosti za to raven.

Na primer, če v primeru zlorab ali nepravilnosti zagotovo nastanejo pravne posledice, je lahko izbrana raven le srednja ali visoka. Če lahko nastane ekonomska škoda, pa so za ta kriterij možne ravni izbire nizka, srednja ali visoka.

Tabela 1: Vrednosti kriterijev in ustrezne ravni zanesljivosti

	Raven zanesljivosti SI-CAS			
Kategorija	Zelo nizka	Nizka	Srednja	Visoka
Pravne posledice	Brez	Mogoče	DA	DA
Pravne zahteve	Brez	N	S	V
Posredovanje osebnih podatkov	ZN	N	S	V
Prikaz osebnih podatkov	ZN	N	S	V
Registri identifikacijskih podatkov	N	N	S	V
Ekonomska škoda	ZN	N	S	V
Javni interes	N	S	S	V
Osebna varnost	ZN	N	S	V

Lastnosti posameznih ravni zanesljivosti so povzete v spodnji tabeli.

Tabela 2: Lastnosti ravni zanesljivosti

Vrednosti kriterijev	**Raven zanesljivosti SI-CAS**
• Brez pravnih posledic • Brez pravnih zahtev • Posredovanje osebnih podatkov kategorije ZN • Prikaz osebnih podatkov kategorije ZN • Brez spreminjanja in kreiranja identifikacijskih podatkov v registrih • Brez ekonomske škode • Javni interes: N • Osebna varnost: ZN	Zelo nizka
• Možne pravne posledice • Zahteva za napredni elektronski podpis • Posredovanje osebnih podatkov kategorij do vrednosti N • Prikaz osebnih podatkov kategorij do vrednosti N • Registri podatkov: N • Ekonomska škoda: N • Javni interes: S • Osebna varnost: N	Nizka
• Pravne posledice • Zahteva za napredni elektronski podpis, overjen s kvalificiranim potrdilom • Posredovanje osebnih podatkov kategorij do vrednosti S • Prikaz osebnih podatkov kategorij do vrednosti S • Registri podatkov: S • Ekonomska škoda: S • Javni interes: S	Srednja

• Osebna varnost: S	
• Pravne posledice • Zahteva za kvalificirani elektronski podpis • Posredovanje osebnih podatkov kategorije V • Prikaz osebnih podatkov kategorije V • Registri podatkov: V • Ekonomska škoda: V • Javni interes: V • Osebna varnost: V	Visoka