PROVEDBENA UREDBA KOMISIJE (EU) 2015/1502

od 8. rujna 2015.

o utvrđivanju minimalnih tehničkih specifikacija i postupaka za razine osiguranja identiteta koje se pripisuju sredstvima elektroničke identifikacije u skladu s člankom 8. stavkom 3. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ ([1]), a posebno njezin članak 8. stavak 3.,

budući da:

(1) Člankom 8. Uredbe (EU) br. 910/2014 predviđeno je da se sustavom elektroničke identifikacije koji je prijavljen na temelju članka 9. stavka 1. treba odrediti niska, značajna i visoka razina osiguranja identiteta koja se pripisuje sredstvima elektroničke identifikacije koja su izdana u okviru tog sustava.

(2) Određivanje minimalnih tehničkih specifikacija, normi i postupaka ključno je kako bi se osiguralo jednako tumačenje pojedinosti o razinama osiguranja identiteta i kako bi se osigurala interoperabilnost pri raspoređivanju nacionalnih razina osiguranja identiteta prijavljenih sustava elektroničke identifikacije u odnosu na razine osiguranja identiteta na temelju članka 8. kako je predviđeno u članku 12. stavku 4. točki (b) Uredbe (EU) br. 910/2014.

(3) Za specifikacije i postupke utvrđene ovim provedbenim aktom uzeta je u obzir međunarodna norma ISO/IEC 29115 kao najrelevantnija međunarodna norma u području razina osiguranja identiteta za sredstva elektroničke identifikacije. Međutim, sadržaj Uredbe (EU) br. 910/2014 razlikuje se od te međunarodne norme, posebno u pogledu zahtjeva za dokazivanje i provjeru identiteta te načina na koji su uzete u obzir razlike između aranžmana za dokazivanje identiteta država članica i postojećih alata u EU-u koji se upotrebljavanju u istu svrhu. Stoga se u Prilogu, premda se on temelji na toj međunarodnoj normi, ne bi smjelo upućivati na bilo koji određeni sadržaj norme ISO/IEC 29115.

(4) Ova je Uredba izrađena na temelju pristupa usmjerenog na rezultate, kao najprikladnijeg pristupa, što se odražava i u definicijama za određivanje pojmova i koncepata. Njima se uzima u obzir cilj Uredbe (EU) br. 910/2014 s obzirom na razine osiguranja identiteta sredstava elektroničke identifikacije. Stoga bi pri određivanju specifikacija i postupaka iz ovog provedbenog akta u najvećoj mjeri trebalo uzeti u obzir opsežni pilot-projekt STORK, uključujući specifikacije razvijene u okviru tog projekta, te definicije i koncepte iz norme ISO/IEC 29115.

(5) Ovisno o kontekstu u kojem je određeni aspekt dokaza o identitetu potrebno provjeriti, mjerodavni izvori mogu imati različite oblike kao što su, među ostalim, registri, dokumenti, tijela. Različite države članice mogu se, čak i u sličnom kontekstu, služiti različitim mjerodavnim izvorima.

(6) Zahtjevima za dokazivanje i provjeru identiteta trebalo bi uzeti u obzir različite sustave i praksu uz dovoljno visoku razinu osiguranja identiteta kako bi se uspostavilo neophodno povjerenje. Stoga bi prihvaćanje postupaka koji su se prethodno upotrebljavali u svrhu različitu od izdavanja sredstava elektroničke identifikacije trebalo biti uvjetovano potvrdom da ti postupci ispunjavaju zahtjeve predviđene za odgovarajuću razinu osiguranja identiteta.

([1]) SL L 257, 28.8.2014., str. 73.

(7) Obično se za to upotrebljavaju određeni čimbenici autentikacije, kao što su zajedničke tajne, fizički uređaji i fizička obilježja. Međutim, trebalo bi poticati uporabu većeg broja čimbenika autentikacije, posebno čimbenika različitih kategorija, kako bi se povećala sigurnost procesa autentikacije.

(8) Ova Uredba ne bi trebala utjecati na prava zastupanja pravnih osoba. Međutim, Prilogom bi trebalo predvidjeti zahtjeve za povezivanje sredstava elektroničke identifikacije fizičkih i pravnih osoba.

(9) Trebalo bi prepoznati važnost sigurnosti informacija i sustava upravljanja uslugama te važnost primjene priznatih metoda i načela ugrađenih u norme, kao što su serije normi ISO/IEC 27000 i ISO/IEC 20000.

(10) Također bi trebalo uzeti u obzir dobru praksu u odnosu na razine osiguranja identiteta u državama članicama.

(11) Certificiranje sigurnosti informacijske tehnologije na temelju međunarodnih normi važan je alat za provjeru ispunjavaju li proizvodi sigurnosne zahtjeve ovog provedbenog akta.

(12) Odbor iz članka 48. Uredbe (EU) br. 910/2014 nije dostavio mišljenje u roku koji je utvrdio njegov predsjednik,

DONIJELA JE OVU UREDBU:

Članak 1.

1. Niska, značajna i visoka razina osiguranja identiteta za sredstva elektroničke identifikacije izdana u okviru prijavljenog sustava elektroničke identifikacije određuju se s obzirom na specifikacije i postupke utvrđene u Prilogu.

2. Specifikacije i postupci utvrđeni u Prilogu upotrebljavaju se za određivanje razine osiguranja identiteta sredstava elektroničke identifikacije izdanih u okviru prijavljenog sustava elektroničke identifikacije određivanjem pouzdanosti i kvalitete sljedećih elemenata:

(a) upis, kako je utvrđeno u odjeljku 2.1. Priloga ovoj Uredbi u skladu s člankom 8. stavkom 3. točkom (a) Uredbe (EU) br. 910/2014;

(b) upravljanje sredstvima elektroničke identifikacije, kako je utvrđeno u odjeljku 2.2. Priloga ovoj Uredbi u skladu s člankom 8. stavkom 3. točkama (b) i (f) Uredbe (EU) br. 910/2014;

(c) autentikacija, kako je utvrđeno u odjeljku 2.3. Priloga ovoj Uredbi u skladu s člankom 8. stavkom 3. točkom (c) Uredbe (EU) br. 910/2014;

(d) upravljanje i organizacija, kako je utvrđeno u odjeljku 2.4. Priloga ovoj Uredbi u skladu s člankom 8. stavkom 3. točkama (d) i (e) Uredbe (EU) br. 910/2014.

3. Kada sredstvo elektroničke identifikacije izdano u okviru prijavljenog sustava elektroničke identifikacije ispunjava zahtjev koji pripada višoj razini osiguranja identiteta, pretpostavlja se da ispunjava jednakovrijedan zahtjev niže razine osiguranja identiteta.

4. Osim ako je drukčije navedeno u odgovarajućem dijelu Priloga, svi elementi navedeni u Prilogu za određenu razinu osiguranja identiteta sredstava elektroničke identifikacije izdanih u okviru prijavljenog sustava elektroničke identifikacije ispunjeni su kako bi odgovarali određenoj razini osiguranja identiteta.

Članak 2.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 8. rujna 2015.

Za Komisiju
Predsjednik
Jean-Claude JUNCKER

PRILOG

Tehničke specifikacije i postupci za nisku, značajnu i visoku razinu osiguranja identiteta za sredstva elektroničke identifikacije izdana u okviru prijavljenog sustava elektroničke identifikacije

1. **Primjenjive definicije**

Za potrebe ovog Priloga primjenjuju se sljedeće definicije:

1. „mjerodavni izvor" znači svaki izvor bez obzira na njegov oblik, koji je pouzdan u pogledu pružanja točnih podataka, informacija i/ili dokaza koji se mogu upotrijebiti za dokazivanje identiteta;

2. „čimbenik autentikacije" znači čimbenik za koji je potvrđeno da je povezan s osobom, a može pripadati jednoj od sljedećih kategorija:

   (a) „čimbenik autentikacije na temelju vlasništva" znači čimbenik autentikacije za koji subjekt mora dokazati da ga posjeduje;

   (b) „čimbenik autentikacije na temelju znanja" znači čimbenik autentikacije za koji subjekt mora dokazati da ga poznaje;

   (c) „svojstveni čimbenik autentikacije" znači čimbenik autentikacije temeljen na fizičkom obilježju fizičke osobe, za koje subjekt mora dokazati da ga posjeduje;

3. „dinamička autentikacija" znači elektronički proces u kojem se upotrebljava kriptografija ili druge tehnike kako bi se na zahtjev stvorio elektronički dokaz da subjekt kontrolira ili posjeduje identifikacijske podatke i koji se mijenja sa svakom autentikacijom između subjekta i sustava koji provjerava identitet subjekta;

4. „sustav upravljanja sigurnošću informacija" znači skup procesa i postupaka osmišljenih kako bi se rizicima koji se odnose na sigurnost informacija upravljalo na prihvatljivim razinama.

2. **Tehničke specifikacije i postupci**

Elementi tehničkih specifikacija i postupaka opisanih u ovom Prilogu upotrebljavaju se za određivanje načina primjene zahtjeva i kriterija iz članka 8. Uredbe (EU) br. 910/2014 na sredstva elektroničke identifikacije izdana u okviru sustava elektroničke identifikacije.

2.1. *Upis*

2.1.1. Zahtjev i registracija

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Osigurati da je podnositelj zahtjeva upoznat s uvjetima povezanima s uporabom sredstava elektroničke identifikacije. 2. Osigurati da je podnositelj zahtjeva upoznat s preporučenim sigurnosnim mjerama opreza povezanima sa sredstvima elektroničke identifikacije. 3. Prikupiti relevantne podatke o identitetu potrebne za dokazivanje i provjeru identiteta.
Značajna	Isto kao za nisku razinu.
Visoka	Isto kao za nisku razinu.

2.1.2. Dokazivanje i provjera identiteta (fizička osoba)

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Može se pretpostavljati da osoba posjeduje dokaz koji je priznala država članica u kojoj se podnosi zahtjev za izdavanje sredstva elektroničke identifikacije i da se njime potvrđuje prijavljeni identitet. 2. Može se pretpostavljati da je dokaz vjerodostojan, odnosno da prema mjerodavnom izvoru postoji te da se čini valjanim. 3. Mjerodavni izvor zna da prijavljeni identitet postoji i može se pretpostavljati da odgovara osobi koja prijavljuje identitet.
Značajna	Niska razina, uz jednu od sljedećih mogućnosti navedenih u točkama 1. do 4.: 1. Provjereno je da osoba posjeduje dokaz koji je priznala država članica u kojoj je zahtjev za izdavanje sredstva elektroničke identifikacije podnesen i da se njime potvrđuje prijavljeni identitet i dokaz se provjerava kako bi se utvrdilo da je vjerodostojan; ili mjerodavni izvor zna da identitet postoji i da se odnosi na pravu osobu i poduzete su mjere kako bi se na najmanju mjeru sveo rizik da identitet osobe ne odgovara prijavljenom identitetu, uzimajući u obzir na primjer rizik od gubitka, krađe, suspenzije, opoziva ili isteka valjanosti dokaza; ili 2. podnesen je identifikacijski dokument tijekom postupka registracije u državi članici u kojoj je dokument bio izdan i čini se da se dokument odnosi na osobu koja ga je podnijela i poduzete su mjere kako bi se na najmanju mjeru sveo rizik da identitet osobe ne odgovara prijavljenom identitetu, uzimajući u obzir na primjer rizik od gubitka, krađe, suspenzije, opoziva ili isteka valjanosti dokumenata; ili 3. ako postupci koje je javni ili privatni subjekt prethodno primjenjivao u istoj državi članici u svrhu različitu od izdavanja sredstava elektroničke identifikacije omogućuju jednaku razinu osiguranja identiteta kao oni utvrđeni u odjeljku 2.1.2. za značajnu razinu osiguranja identiteta, subjekt nadležan za registraciju ne mora ponavljati prethodne postupke, pod uvjetom da takvu jednakovrijednu razinu osiguranja identiteta potvrdi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 Europskog parlamenta i Vijeća ([1]) ili jednakovrijedno tijelo; ili 4. ako se sredstva elektroničke identifikacije izdaju na temelju valjanih prijavljenih sredstava elektroničke identifikacije koja imaju značajnu ili visoku razinu osiguranja identiteta te ako se njima uzimaju u obzir rizici od promjene osobnih identifikacijskih podataka, nije potrebno ponoviti postupke dokazivanja i provjere identiteta. Ako sredstva elektroničke identifikacije koja služe kao temelj za izdavanje nisu prijavljena, značajnu ili visoku razinu osiguranja identiteta mora potvrditi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo.

Razina osiguranja identiteta	Potrebni elementi
Visoka	Moraju biti ispunjeni zahtjevi iz točke 1. ili 2.: 1. Značajna razina, uz jednu od sljedećih mogućnosti navedenih u točkama (a) do (c): (a) Ako je provjereno da osoba posjeduje fotografski ili biometrijski identifikacijski dokaz koji je priznala država članica u kojoj je zahtjev za izdavanje sredstva elektroničke identifikacije podnesen i da podneseni dokaz predstavlja prijavljeni identitet, dokaz se provjerava kako bi se utvrdilo da je valjan prema mjerodavnom izvoru i usporedbom jedne fizičke karakteristike osobe ili više njih s mjerodavnim izvorom utvrđeno je da podnositelj zahtjeva odgovara prijavljenom identitetu; ili (b) ako postupci koje je javni ili privatni subjekt prethodno primjenjivao u istoj državi članici u svrhu različitu od izdavanja sredstava elektroničke identifikacije omogućuju jednaku razinu osiguranja identiteta kao oni utvrđeni u odjeljku 2.1.2. za visoku razinu osiguranja identiteta, subjekt nadležan za registraciju ne mora ponavljati prethodne postupke, pod uvjetom da takvu jednakovrijednu razinu osiguranja identiteta potvrdi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo i poduzete su mjere kako bi se dokazalo da su rezultati prethodnih postupaka i dalje valjani; ili (c) ako se sredstva elektroničke identifikacije izdaju na temelju valjanih prijavljenih sredstava elektroničke identifikacije koja imaju visoku razinu osiguranja identiteta te ako se njima uzimaju u obzir rizici od promjene osobnih identifikacijskih podataka, nije potrebno ponoviti postupke dokazivanja i provjere identiteta. Ako sredstva elektroničke identifikacije koja služe kao temelj za izdavanje nisu prijavljena, visoku razinu osiguranja identiteta mora potvrditi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo i poduzete su mjere kako bi se dokazalo da su rezultati tog prethodnog postupka izdavanja prijavljenog sredstva elektroničke identifikacije i dalje valjani; ili 2. ako podnositelj zahtjeva ne podnese priznati fotografski ili biometrijski identifikacijski dokaz, primjenjuju se isti postupci koji se primjenjuju na nacionalnoj razini u državi članici subjekta nadležnog za registraciju za dobivanje takvog priznatog fotografskog ili biometrijskog identifikacijskog dokaza.

([1]) Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).

2.1.3. Dokazivanje i provjera identiteta (pravna osoba)

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Prijavljeni identitet pravne osobe dokazuje se na temelju dokaza koje je priznala država članica u kojoj je zahtjev za izdavanje sredstva elektroničke identifikacije podnesen.

Razina osiguranja identiteta	Potrebni elementi
	2. Dokazi se čine valjanima i može se pretpostavljati da su vjerodostojni odnosno da postoje prema mjerodavnom izvoru, ako je uključenje pravne osobe u mjerodavni izvor dobrovoljno i uređeno je dogovorom između pravne osobe i mjerodavnog izvora. 3. Prema saznanjima mjerodavnog izvora fizička osoba nema status koji bi joj priječio da djeluje u ime pravne osobe.
Značajna	Niska razina, uz jednu od sljedećih mogućnosti navedenih u točkama 1. do 3.: 1. Prijavljeni identitet pravne osobe dokazuje se na temelju dokaza koje je priznala država članica u kojoj je zahtjev za izdavanje sredstva elektroničke identifikacije podnesen, uključujući ime pravne osobe, pravni oblik i (prema potrebi) njezin registracijski broj i dokazi se provjeravaju kako bi se utvrdilo jesu li vjerodostojni odnosno da postoje prema mjerodavnom izvoru, ako je uključenje pravne osobe u mjerodavni izvor potrebno kako bi pravna osoba djelovala u svojem sektoru i poduzete su mjere kako bi se na najmanju mjeru sveo rizik da identitet osobe ne odgovara prijavljenom identitetu, uzimajući u obzir na primjer rizik od gubitka, krađe, suspenzije, opoziva ili isteka valjanosti dokumenata; ili 2. ako postupci koje je javni ili privatni subjekt prethodno primjenjivao u istoj državi članici u svrhu različitu od izdavanja sredstava elektroničke identifikacije omogućuju jednaku razinu osiguranja identiteta kao oni utvrđeni u odjeljku 2.1.3. za značajnu razinu osiguranja identiteta, subjekt nadležan za registraciju ne mora ponavljati prethodne postupke, pod uvjetom da takvu jednakovrijednu razinu osiguranja identiteta potvrdi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo; ili 3. ako se sredstva elektroničke identifikacije izdaju na temelju valjanih prijavljenih sredstava elektroničke identifikacije koja imaju značajnu ili visoku razinu osiguranja identiteta, nije potrebno ponoviti procese dokazivanja i provjere identiteta. Ako sredstva elektroničke identifikacije koja služe kao temelj za izdavanje nisu prijavljena, značajnu ili visoku razinu osiguranja identiteta mora potvrditi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo.
Visoka	Značajna razina, uz jednu od sljedećih mogućnosti navedenih u točkama 1. do 3.: 1. Prijavljeni identitet pravne osobe dokazuje se na temelju dokaza koje je priznala država članica u kojoj je zahtjev za izdavanje sredstva elektroničke identifikacije podnesen, uključujući ime pravne osobe, pravni oblik i barem jedan jedinstveni identifikator koji predstavlja pravnu osobu i koji se upotrebljava u nacionalnom kontekstu i dokazi se provjeravaju kako bi se utvrdilo da su valjani prema mjerodavnom izvoru; ili

Razina osiguranja identiteta	Potrebni elementi
	2. ako postupci koje je javni ili privatni subjekt prethodno primjenjivao u istoj državi članici u svrhu različitu od izdavanja sredstava elektroničke identifikacije omogućuju jednaku razinu osiguranja identiteta kao oni utvrđeni u odjeljku 2.1.3. za visoku razinu osiguranja identiteta, subjekt nadležan za registraciju ne mora ponavljati prethodne postupke, pod uvjetom da takvu jednakovrijednu razinu osiguranja identiteta potvrdi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo i poduzete su mjere kako bi se dokazalo da su rezultati tog prethodnog postupka i dalje valjani; ili 3. ako se sredstva elektroničke identifikacije izdaju na temelju valjanih prijavljenih sredstava elektroničke identifikacije koja imaju visoku razinu osiguranja identiteta, nije potrebno ponoviti postupke dokazivanja i provjere identiteta. Ako sredstva elektroničke identifikacije koja služe kao temelj za izdavanje nisu prijavljena, visoku razinu osiguranja identiteta mora potvrditi tijelo za ocjenjivanje sukladnosti iz članka 2. stavka 13. Uredbe (EZ) br. 765/2008 ili jednakovrijedno tijelo i poduzete su mjere kako bi se dokazalo da su rezultati tog prethodnog postupka izdavanja prijavljenog sredstva elektroničke identifikacije i dalje valjani.

2.1.4. Povezivanje sredstava elektroničke identifikacije fizičkih i pravnih osoba

Prema potrebi, na povezivanje sredstava elektroničke identifikacije fizičkih osoba sa sredstvima elektroničke identifikacije pravnih osoba („povezivanje”) primjenjuju se sljedeći uvjeti:

1. Povezivanje se može suspendirati ili opozvati. Životnim ciklusom povezivanja (npr. aktivacija, suspenzija, obnova, opoziv) upravlja se u skladu s priznatim postupcima na nacionalnoj razini.

2. Fizička osoba čija su sredstva elektroničke identifikacije povezana sa sredstvima elektroničke identifikacije pravne osobe može delegirati izvršavanje povezivanja drugoj fizičkoj osobi na temelju priznatih postupaka na nacionalnoj razini. Međutim, odgovornost i dalje snosi fizička osoba koja delegira.

3. Povezivanje se obavlja na sljedeći način:

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Provjerava se da je dokazivanje identiteta fizičke osobe koja djeluje u ime pravne osobe bilo izvršeno na niskoj ili na višoj razini. 2. Povezivanje je uspostavljeno na temelju priznatih postupaka na nacionalnoj razini. 3. Prema saznanjima mjerodavnog izvora fizička osoba nema status koji bi joj priječio da djeluje u ime pravne osobe.
Značajna	Točka 3. niske razine, uz sljedeće elemente: 1. Provjerava se da je dokazivanje identiteta fizičke osobe koja djeluje u ime pravne osobe bilo izvršeno na značajnoj ili visokoj razini.

Razina osiguranja identiteta	Potrebni elementi
	2. Povezivanje je uspostavljeno na temelju priznatih postupaka na nacionalnoj razini, što je dovelo do registracije povezivanja u mjerodavnom izvoru. 3. Povezivanje je provjereno na temelju informacija koje potječu od mjerodavnog izvora.
Visoka	Točka 3. niske razine i točka 2. značajne razine, uz sljedeće elemente: 1. Provjerava se da je dokazivanje identiteta fizičke osobe koja djeluje u ime pravne osobe bilo izvršeno na visokoj razini. 2. Povezivanje je provjereno na temelju jedinstvenog identifikatora koji predstavlja pravnu osobu i koji se upotrebljava u nacionalnom kontekstu te na temelju informacija iz mjerodavnog izvora koje nedvojbeno predstavljaju fizičku osobu.

2.2. *Upravljanje sredstvima elektroničke identifikacije*

2.2.1. Karakteristike i dizajn sredstava elektroničke identifikacije

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Sredstvo elektroničke identifikacije upotrebljava barem jedan čimbenik autentikacije. 2. Dizajn sredstva elektroničke identifikacije takav je da izdavatelj poduzima razumne mjere kako bi utvrdio da se ono upotrebljava samo pod kontrolom ili u vlasništvu osobe kojoj pripada.
Značajna	1. Sredstvo elektroničke identifikacije upotrebljava barem dva čimbenika autentikacije različitih kategorija. 2. Dizajn sredstva elektroničke identifikacije takav je da se može pretpostaviti da se ono upotrebljava samo pod kontrolom ili u vlasništvu osobe kojoj pripada.
Visoka	Značajna razina, uz sljedeće elemente: 1. Sredstvo elektroničke identifikacije štiti od kopiranja i neovlaštene izmjene te od napadača s velikim napadačkim potencijalom. 2. Dizajn sredstva elektroničke identifikacije takav je da ga osoba u čijem je vlasništvu može pouzdano zaštititi od uporabe drugih osoba.

2.2.2. Izdavanje, dostava i aktivacija

Razina osiguranja identiteta	Potrebni elementi
Niska	Nakon izdavanja, sredstvo elektroničke identifikacije isporučuje se s pomoću mehanizma za koji se pretpostavlja da osigurava isporuku samo osobi kojoj je sredstvo namijenjeno.
Značajna	Nakon izdavanja, sredstvo elektroničke identifikacije isporučuje se s pomoću mehanizma za koji se pretpostavlja da osigurava isporuku samo u vlasništvo osobe koja je vlasnik.
Visoka	Procesom aktiviranja provjerava se da je sredstvo elektroničke identifikacije isporučeno samo u vlasništvo osobe koja je vlasnik.

2.2.3. Suspenzija, opoziv i ponovna aktivacija

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Sredstvo elektroničke identifikacije može se pravovremeno i učinkovito suspendirati i/ili opozvati. 2. Postoje mjere koje se poduzimaju kako bi se spriječila neovlaštena suspenzija, opoziv i/ili ponovna aktivacija. 3. Do ponovne aktivacije dolazi samo ako su i dalje ispunjeni isti zahtjevi za sigurnost utvrđeni prije suspenzije ili opoziva.
Značajna	Isto kao za nisku razinu.
Visoka	Isto kao za nisku razinu.

2.2.4. Obnova i zamjena

Razina osiguranja identiteta	Potrebni elementi
Niska	Uzimajući u obzir rizike od promjene osobnih identifikacijskih podataka, obnova ili zamjena mora ispunjavati iste zahtjeve kao i prvotno dokazivanje i provjera identiteta ili se temelji na valjanom sredstvu elektroničke identifikacije iste ili više razine osiguranja identiteta.
Značajna	Isto kao za nisku razinu.
Visoka	Niska razina, uz sljedeće elemente: Ako se obnova ili zamjena temelje na valjanom sredstvu elektroničke identifikacije, podaci o identitetu provjeravaju se s mjerodavnim izvorom.

2.3. *Autentikacija*

Ovaj odjeljak usredotočuje se na opasnosti povezane s uporabom mehanizma autentikacije i u njemu se navode zahtjevi za svaku razinu osiguranja identiteta. Za potrebe ovog odjeljka smatra se da kontrole odgovaraju rizicima na određenoj razini.

2.3.1. Mehanizam autentikacije

U sljedećoj tablici utvrđeni su zahtjevi prema razini osiguranja identiteta u odnosu na mehanizam autentikacije s pomoću kojeg fizička ili pravna osoba upotrebljava sredstva elektroničke identifikacije za potvrđivanje svojeg identiteta pouzdajućoj strani.

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Otkrivanju osobnih identifikacijskih podataka prethodi pouzdana provjera sredstva elektroničke identifikacije i njegove valjanosti. 2. Ako se osobni identifikacijski podaci pohranjuju kao dio mehanizma autentikacije, te su informacije zaštićene od gubitka i ugroze, uključujući izvanmrežnu analizu. 3. Mehanizmom autentikacije provode se zaštitne kontrole za provjeru sredstava elektroničke identifikacije, tako da je malo vjerojatno da bi aktivnosti napadača s pojačanim osnovnim napadačkim potencijalom, kao što je pogađanje zaporki, prisluškivanje, ponovno slanje ili manipuliranje komunikacijom, mogle ugroziti mehanizam autentikacije.

Razina osiguranja identiteta	Potrebni elementi
Značajna	Niska razina, uz sljedeće elemente: 1. Otkrivanju osobnih identifikacijskih podataka prethodi pouzdana provjera sredstva elektroničke identifikacije i njegove valjanosti s pomoću dinamičke autentikacije. 2. Mehanizmom autentikacije provode se zaštitne kontrole za provjeru sredstava elektroničke identifikacije, tako da je malo vjerojatno da bi aktivnosti napadača s umjerenim napadačkim potencijalom, kao što je pogađanje zaporki, prisluškivanje, ponovno slanje ili manipuliranje komunikacijom, mogle ugroziti mehanizam autentikacije.
Visoka	Značajna razina, uz sljedeće elemente: Mehanizmom autentikacije provode se zaštitne kontrole za provjeru sredstava elektroničke identifikacije, tako da je malo vjerojatno da bi aktivnosti napadača, kao što je pogađanje zaporki, prisluškivanje, ponovno slanje ili manipuliranje komunikacijom, mogle ugroziti mehanizam autentikacije.

2.4. *Upravljanje i organizacija*

Svi sudionici koji pružaju usluge povezane s elektroničkom identifikacijom u prekograničnom kontekstu („pružatelji usluga”) uspostavljaju praksu upravljanja sigurnošću dokumentiranih informacija, politike, pristupe upravljanju rizikom i druge priznate kontrole kako bi zajamčili tijelima za upravljanje sustavima elektroničke identifikacije u predmetnim državama članicama da postoji učinkovita praksa. Za potrebe cijelog odjeljka 2.4. smatra se da svi zahtjevi/elementi odgovaraju rizicima na određenoj razini.

2.4.1. Opće odredbe

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Pružatelji usluga koji isporučuju bilo koju operativnu uslugu obuhvaćenu ovom Uredbom jesu javno tijelo ili pravni subjekt priznat kao takav na temelju nacionalnog prava države članice koji ima uspostavljenu organizaciju i koji je potpuno funkcionalan u svim dijelovima mjerodavnima za pružanje usluga. 2. Pružatelji usluga ispunjavaju sve zakonske zahtjeve propisane u vezi s funkcioniranjem i isporukom usluga, uključujući vrste informacija koje se mogu tražiti, način na koji se provodi dokazivanje identiteta, koje se informacije mogu zadržati i koliko dugo. 3. Pružatelji usluga mogu dokazati da su sposobni preuzeti rizik od odgovornosti za štetu i da imaju dostatna financijska sredstva za neprekinuto funkcioniranje i pružanje usluga. 4. Pružatelji usluga odgovorni su za ispunjenje svih obveza izdvojenih drugom subjektu i usklađenost s politikom programa, kao da su sami ispunili te zadaće. 5. Sustavi elektroničke identifikacije koji nisu obuhvaćeni nacionalnim pravom imaju uspostavljen učinkovit plan prekida. Takav plan uključuje da se pružanje usluge pravovremeno prekine ili da uslugu nastavi pružati drugi pružatelj usluga te način na koji se obavješćuju mjerodavna tijela i krajnji korisnici i pojedinosti o načinu na koji se štite, čuvaju i uništavaju evidencije u skladu s općim pravilima programa.
Značajna	Isto kao za nisku razinu.
Visoka	Isto kao za nisku razinu.

2.4.2. Objavljene obavijesti i informacije za korisnike

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Objavljena je definicija usluge koja uključuje sve primjenjive uvjete i naknade, uključujući sva ograničenja njezine uporabe. Definicija usluge uključuje politiku zaštite privatnosti. 2. Uspostavljaju se odgovarajuća politika i postupci kako bi se osiguralo da su korisnici usluge pravovremeno i pouzdano informirani o promjenama definicije usluge i svih primjenjivih uvjeta te politike zaštite privatnosti za određenu uslugu. 3. Uspostavljaju se odgovarajuće politike i postupci kako bi se omogućilo davanje potpunih i ispravnih odgovora na zahtjeve za informacije.
Značajna	Isto kao za nisku razinu.
Visoka	Isto kao za nisku razinu.

2.4.3. Upravljanje sigurnošću informacija

Razina osiguranja identiteta	Potrebni elementi
Niska	Postoji učinkovit sustav upravljanja sigurnošću informacija za kontrolu rizika povezanih sa sigurnošću informacija i upravljanje njima.
Značajna	Niska razina, uz sljedeće elemente: Sustav upravljanja sigurnošću informacija u skladu je s dokazanim normama ili načelima za kontrolu rizika povezanih sa sigurnošću informacija i upravljanje njima.
Visoka	Isto kao za značajnu razinu.

2.4.4. Vođenje evidencije

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Vođenje evidencije i zadržavanje relevantnih informacija uporabom učinkovitog sustava za upravljanje evidencijom, uzimajući u obzir primjenjivo zakonodavstvo i dobru praksu u odnosu na zaštitu podataka i zadržavanje podataka. 2. Zadržavanje, u mjeri u kojoj se to dopušta u okviru nacionalnog prava ili drugog nacionalnog administrativnog aranžmana, i zaštita evidencije koliko god je to potrebno za potrebe revizije i istrage o kršenju sigurnosti te zadržavanja podataka, nakon čega se evidencija mora sigurno uništiti.
Značajna	Isto kao za nisku razinu.
Visoka	Isto kao za nisku razinu.

2.4.5. Objekti i osoblje

Sljedeća tablica prikazuje zahtjeve povezane s objektima, osobljem i podizvođačima, ako je primjenjivo, koji obavljaju dužnosti obuhvaćene ovom Uredbom. Usklađenost sa zahtjevima razmjerna je razini rizika povezanoj s pruženom razinom osiguranja identiteta.

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Postoje postupci kojima se osigurava da su osoblje i podizvođači dovoljno obučeni i kvalificirani te da imaju dovoljno iskustva u vještinama potrebnima za obavljanje svoje uloge. 2. Angažirano je dovoljno osoblja i podizvođača za primjereno obavljanje usluge i osiguravanje resursa u skladu s relevantnim politikama i postupcima. 3. Objekti koji se upotrebljavaju za pružanje usluge neprestano se nadziru i štite od štete uzrokovane vremenskim uvjetima, neovlaštenog pristupa i drugih čimbenika koji mogu utjecati na sigurnost usluge. 4. Objekti koji se upotrebljavaju za pružanje usluge omogućuju da je pristup područjima u kojima se nalaze ili se obrađuju osobni, kriptografski ili drugi osjetljivi podaci moguć samo ovlaštenom osoblju ili podizvođačima.
Značajna	Isto kao za nisku razinu.
Visoka	Isto kao za nisku razinu.

2.4.6. Tehničke kontrole

Razina osiguranja identiteta	Potrebni elementi
Niska	1. Postoje razmjerne tehničke kontrole za upravljanje rizicima za sigurnost usluga kojima se štiti povjerljivost, cjelovitost i dostupnost informacija koje se obrađuju. 2. Elektronički komunikacijski kanali koji se upotrebljavaju za razmjenu osobnih ili osjetljivih informacija zaštićeni su od prisluškivanja, manipulacije i ponovnog slanja. 3. Pristup osjetljivom kriptografskom materijalu, ako se upotrebljava za izdavanje sredstava elektroničke identifikacije i autentikaciju, ograničen je na uloge i aplikacije za koje se taj pristup izričito zahtijeva. Osigurava se da takav materijal nikad nije kontinuirano pohranjen u formatu običnog teksta. 4. Postoje postupci kako bi se osiguralo da se sigurnost održava kroz vrijeme i da je sustav sposoban odgovoriti na promjene razina rizika, incidente i kršenja sigurnosti. 5. Svi mediji koji sadržavaju osobne, kriptografske ili druge osjetljive informacije skladište se, prevoze i uništavaju na siguran način.
Značajna	Isto kao za nisku razinu, uz sljedeće elemente: Osjetljivi kriptografski materijal, ako se upotrebljava za izdavanje sredstava elektroničke identifikacije i autentikaciju, zaštićen je od neovlaštene izmjene.
Visoka	Isto kao za značajnu razinu.

2.4.7. Usklađenost i revizija

Razina osiguranja identiteta	Potrebni elementi
Niska	Postoje periodične unutarnje revizije kojima su obuhvaćeni svi dijelovi koji se odnose na isporuku usluga koje se pružaju kako bi se osigurala usklađenost s relevantnom politikom.

Razina osiguranja identiteta	Potrebni elementi
Značajna	Postoje periodične neovisne unutarnje ili vanjske revizije kojima su obuhvaćeni svi dijelovi koji se odnose na isporuku usluga koje se pružaju kako bi se osigurala usklađenost s relevantnom politikom.
Visoka	1. Postoje periodične neovisne vanjske revizije kojima su obuhvaćeni svi dijelovi koji se odnose na isporuku usluga koje se pružaju kako bi se osigurala usklađenost s relevantnom politikom. 2. Ako programom izravno upravlja državno tijelo, revizija se provodi u skladu s nacionalnim pravom.