

IZVEDBENA UREDBA KOMISIJE (EU) 2015/1502**z dne 8. septembra 2015****o določitvi minimalnih tehničnih specifikacij in postopkov za ravni zanesljivosti za sredstva elektronske identifikacije v skladu s členom 8(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu****(Besedilo velja za EGP)**

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju 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 o razveljavitvi Direktive 1999/93/ES ⁽¹⁾ ter zlasti člena 8(3) Uredbe,

ob upoštevanju naslednjega:

- (1) Člen 8 Uredbe (EU) št. 910/2014 določa, da mora shema elektronske identifikacije, priglášena v skladu s členom 9(1), določati nizko, srednjo in visoko raven zanesljivosti, dodeljeno sredstvom elektronske identifikacije, izdanim v okviru navedene sheme.
- (2) Določitev minimalnih tehničnih specifikacij, standardov in postopkov je bistvena, da se zagotovita skupno razumevanje podrobnih podatkov o ravneh zanesljivosti in interoperabilnost, kadar se določajo nacionalne ravni zanesljivosti priglášenih shem elektronske identifikacije glede na ravni zanesljivosti iz člena 8, kakor določa člen 12(4)(b) Uredbe (EU) št. 910/2014.
- (3) Mednarodni standard ISO/IEC 29115 je bil upoštevan kot glavni razpoložljivi mednarodni standard na področju ravni zanesljivosti za sredstva elektronske identifikacije za specifikacije in postopke iz tega izvedbenega akta. Vendar pa se vsebina Uredbe (EU) št. 910/2014 razlikuje od navedenega mednarodnega standarda, zlasti v zvezi z zahtevami glede dokazovanja in preverjanja identitete ter načina, kako se upoštevajo razlike med ureditvijo identitete v državah članicah in obstoječimi instrumenti EU za isti namen. Zato se Priloga kljub opiranju na ta mednarodni standard ne bi smela sklicevati na katero koli posebno vsebino ISO/IEC 29115.
- (4) Podlaga za pripravo te uredbe je bil na rezultatih temelječi pristop, ki se je izkazal za najprimernejši, kar se odraža tudi v opredelitvah, ki se uporabljajo za podrobno določanje terminov in pojmov. V njih se upošteva cilj Uredbe (EU) št. 910/2014 glede ravni zanesljivosti sredstev elektronske identifikacije. Zato bi bilo treba pri pripravi specifikacij in postopkov iz tega izvedbenega akta dosledno upoštevati obsežni pilotni projekt STORK, vključno s specifikacijami, ki so bile razvite v njegovem okviru, in opredelitve ter pojme iz ISO/IEC 29115.
- (5) Verodostojni viri so lahko glede na okoliščine, v katerih je treba preveriti vidik dokazila o identiteti, v številnih oblikah, kot so med drugim registri, dokumenti in organi. V različnih državah članicah se verodostojni viri lahko razlikujejo celo v podobnih okoliščinah.
- (6) Zahteve za dokazovanje in preverjanje identitete bi morale upoštevati različne sisteme in prakse ter hkrati zagotavljati dovolj visoko zanesljivost, da se vzpostavi potrebno zaupanje. Zato bi sprejetje postopkov, ki so se predhodno uporabljali za druge namene, kot je izdajanje sredstev elektronske identifikacije, moralo biti pogojeno s potrditvijo, da navedeni postopki izpolnjujejo zahteve, ki so določene za ustrezno raven zanesljivosti.

⁽¹⁾ UL L 257, 28.8.2014, str. 73.

- (7) Navadno se uporabljajo določeni dejavniki avtentikacije, kot so deljene skrivnosti, fizične naprave in fizične značilnosti. Vendar bi bilo treba spodbujati uporabo večjega števila dejavnikov avtentikacije, zlasti iz različnih kategorij dejavnikov, da se poveča varnost postopka avtentikacije.
- (8) Ta uredba ne bi smela vplivati na pravice zastopanja pravnih oseb. Vendar bi morale biti v Prilogi določene zahteve za povezavo med sredstvi elektronske identifikacije fizičnih in pravnih oseb.
- (9) Priznati bi bilo treba pomen sistemov informacijske varnosti in upravljanja storitev ter pomen uporabe priznanih metodologij in uporabe načel, ki jih vsebujejo standardi serij ISO/IEC 27000 in ISO/IEC 20000.
- (10) Upoštevati bi bilo treba tudi dobre prakse glede ravni zanesljivosti v državah članicah.
- (11) Izdajanje varnostnih potrdil, kar zadeva informacijsko tehnologijo, na podlagi mednarodnih standardov je pomemben instrument za preverjanje varnostne skladnosti izdelkov z zahtevami iz tega izvedbenega akta.
- (12) Odbor iz člena 48 Uredbe (EU) št. 910/2014 ni dal mnenja v roku, ki ga je določil njegov predsednik –

SPREJELA NASLEDNJO UREDBO:

Člen 1

1. Nizka, srednja in visoka raven zanesljivosti sredstev elektronske identifikacije, izdanih v okviru priglašene sheme elektronske identifikacije, se določi s sklicevanjem na specifikacije in postopke, ki so določeni v Prilogi.
2. Specifikacije in postopki iz Priloge se uporabljajo za podrobno določitev ravni zanesljivosti sredstev elektronske identifikacije, izdanih v okviru priglašene sheme elektronske identifikacije, tako da se določi zanesljivost in kakovost naslednjih elementov:
 - (a) prijava, kakor je določena v oddelku 2.1 Priloge k tej uredbi v skladu s členom 8(3)(a) Uredbe (EU) št. 910/2014;
 - (b) upravljanje sredstva elektronske identifikacije, kakor je določeno v oddelku 2.2 Priloge k tej uredbi v skladu s členom 8(3)(b) in (f) Uredbe (EU) št. 910/2014;
 - (c) avtentikacija, kakor je določena v oddelku 2.3 Priloge k tej uredbi v skladu s členom 8(3)(c) Uredbe (EU) št. 910/2014;
 - (d) upravljanje in organizacija, kakor sta določena v oddelku 2.4 Priloge k tej uredbi v skladu s členom 8(3)(d) in (e) Uredbe (EU) št. 910/2014.
3. Kadar sredstvo elektronske identifikacije, izdano na podlagi priglašene sheme elektronske identifikacije, izpolnjuje zahtevo, navedeno za višjo raven zanesljivosti, se šteje, da izpolnjuje enakovredno zahtevo nižje ravni zanesljivosti.
4. Če ni določeno drugače v ustreznem delu Priloge, morajo biti za doseganje navedene ravni zanesljivosti sredstva elektronske identifikacije, izdanega na podlagi priglašene sheme elektronske identifikacije, izpolnjeni vsi elementi iz Priloge za določeno raven zanesljivosti.

Člen 2

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 8. septembra 2015

Za Komisijo
Predsednik
Jean-Claude JUNCKER

PRILOGA

Tehnične specifikacije in postopki za nizko, srednjo in visoko raven zanesljivosti sredstev elektronske identifikacije, izdanih na podlagi priglašene sheme elektronske identifikacije**1. Opredelitev uporabljenih pojmov**

V tej prilogi se uporabljajo naslednje opredelitve pojmov:

1. „verodostojni vir“ pomeni kateri koli vir v poljubni obliki, ki na zanesljiv način zagotavlja natančne podatke, informacije in/ali dokaze, ki se lahko uporabljajo za dokazovanje identitete;
2. „dejavnik avtentikacije“ pomeni dejavnik, ki je dokazljivo povezan z osebo, in spada v (najmanj) eno izmed naslednjih kategorij:
 - (a) „dejavnik avtentikacije, ki temelji na posesti“ pomeni dejavnik avtentikacije, za katerega mora oseba dokazati, da ga ima v posesti;
 - (b) „dejavnik avtentikacije, ki temelji na poznavanju“ pomeni dejavnik avtentikacije, za katerega mora oseba dokazati, da ga pozna;
 - (c) „inherentni dejavnik avtentikacije“ pomeni dejavnik avtentikacije, ki temelji na fizični značilnosti fizične osebe in v zvezi s katerim mora oseba dokazati, da ima navedeno fizično značilnost;
3. „dinamična avtentikacija“ pomeni elektronski postopek, ki z uporabo kriptografskih ali drugih metod na zahtevo ustvari elektronski dokaz, da ima oseba pod nadzorom ali v posesti identifikacijske podatke, in ki se spremeni z vsako avtentikacijo med osebo in sistemom, ki preverja identiteto osebe;
4. „sistem za upravljanje informacijske varnosti“ pomeni niz procesov in postopkov za upravljanje tveganj v zvezi z informacijsko varnostjo na sprejemljivih ravneh.

2. Tehnične specifikacije in postopki

Elementi tehničnih specifikacij in postopkov iz te priloge se uporabljajo za določanje, kako se zahteve in merila iz člena 8 Uredbe (EU) št. 910/2014 uporabljajo za sredstva elektronske identifikacije, izdana na podlagi sheme elektronske identifikacije.

2.1 Prijava**2.1.1 Vloga in registracija**

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Zagotovljeno je, da vložnik pozna pogoje v zvezi z uporabo sredstev elektronske identifikacije. 2. Zagotovljeno je, da vložnik pozna priporočene previdnostne varnostne ukrepe v zvezi s sredstvi elektronske identifikacije. 3. Zbirajo se ustrezni identifikacijski podatki za dokazovanje in preverjanje identitete.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.1.2 Dokazovanje in preverjanje identitete (fizična oseba)

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Domneva se lahko, da ima oseba v posesti dokaz, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, in predstavlja identiteto, ki se izkazuje. 2. Domneva se lahko, da je dokaz pristen ali da obstaja v skladu z verodostojnim virom in je domnevno veljaven. 3. Verodostojnemu viru je znano, da izkazana identiteta obstaja in domneva se lahko, da gre za isto osebo, ki izkazuje identiteto.
Srednja	<p>Poleg ravni „Nizka“ mora biti izpolnjena še ena izmed možnosti iz točk 1 do 4:</p> <ol style="list-style-type: none"> 1. preverjeno je, da ima oseba v posesti dokaz, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, in predstavlja identiteto, ki se izkazuje; in preverja se pristnost dokaza; ali pa je verodostojnemu viru znano, da dokaz obstaja in se nanaša na resnično osebo; ter sprejeti so bili ukrepi za zmanjšanje tveganja, da identiteta osebe ni enaka identiteti, ki se izkazuje, pri čemer je bilo upoštevano na primer tveganje izgube, kraje, začasne razveljavitve, preklica ali izteka veljavnosti dokaza; ali 2. med postopkom registracije je bil predložen identifikacijski dokument v državi članici, ki ga je izdala, in se nanaša na osebo, ki ga je predložila; in sprejeti so bili ukrepi za zmanjšanje tveganja, da identiteta osebe ni enaka identiteti, ki se izkazuje, pri čemer so bila upoštevana na primer tveganja izgube, kraje, začasne razveljavitve, preklica ali izteka veljavnosti dokumentov; ali 3. kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.2 za srednjo raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 Evropskega parlamenta in Sveta ⁽¹⁾ ali enakovredni organ; ali 4. kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašene sredstva elektronske identifikacije s srednjo ali visoko ravno zanesljivosti in ob upoštevanju tveganj za spremembo identifikacijskih podatkov osebe, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora srednjo in visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ.

Raven zanesljivosti	Zahtevani elementi
Visoka	<p>Izpolnjene morajo biti zahteve iz točke 1 ali 2:</p> <p>1. poleg ravni „Srednja“ mora biti izpolnjena še ena izmed možnosti iz točk (a) do (c):</p> <p>(a) kadar ima oseba preverjeno v posesti dokaz v obliki fotografije ali biometrične identifikacije, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, in navedeni dokaz predstavlja identiteto, ki se izkazuje, se dokaz preveri, da se ugotovi njegova veljavnost v skladu z verodostojnim virom;</p> <p>in</p> <p>s primerjavo ene ali več fizičnih značilnosti osebe z verodostojnim virom je bila izkazana identiteta vložnika;</p> <p>ali</p> <p>(b) kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.2 za visoko raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ;</p> <p>in</p> <p>sprejeti so bili ukrepi za dokazovanje, da so rezultati predhodnih postopkov še vedno veljavni;</p> <p>ali</p> <p>(c) kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašenega sredstva elektronske identifikacije z visoko ravno zanesljivosti in ob upoštevanju tveganj za spremembo identifikacijskih podatkov osebe, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ;</p> <p>in</p> <p>sprejeti so bili ukrepi za dokazovanje, da so rezultati predhodnega postopka za izdajo priglašenega sredstva elektronske identifikacije še vedno veljavni;</p> <p>ALI</p> <p>2. kadar vložnik ne predloži priznanega dokaza s fotografijo ali biometrično identifikacijo, se uporabljajo enaki postopki za pridobitev takega priznanega dokaza s fotografijo ali biometrično identifikacijo kot na nacionalni ravni v državi članici subjekta, ki je odgovoren za registracijo.</p>
<p>(¹) Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).</p>	

2.1.3 Dokazovanje in preverjanje identitete (pravna oseba)

Raven zanesljivosti	Zahtevani elementi
Nizka	<p>1. Identiteta pravne osebe, ki se izkazuje, je dokazana na podlagi dokaza, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije.</p>

Raven zanesljivosti	Zahtevani elementi
	<p>2. Dokaz je domnevno veljaven in lahko se domneva, da je pristen ali da obstaja v skladu z verodostojnim virom, pod pogojem, da je vključitev pravne osebe v verodostojni vir prostovoljna in jo ureja dogovor med pravno osebo in verodostojnim virom.</p> <p>3. Verodostojnemu viru ni znano, da bi bila pravna oseba v stanju, ki bi ji onemogočalo, da deluje kot navedena pravna oseba.</p>
Srednja	<p>Poleg ravni „Nizka“ mora biti izpolnjena še ena izmed možnosti iz točk 1 do 3:</p> <p>1. identiteta pravne osebe, ki se izkazuje, je dokazana na podlagi dokaza, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, vključno z imenom pravne osebe, pravno obliko in (kadar se uporablja) registracijsko številko;</p> <p>in</p> <p>preverja se pristnost dokaza, ali je njegov obstoj znan verodostojnemu viru, kadar se zahteva vključitev pravne osebe v verodostojni vir za delovanje znotraj njenega sektorja;</p> <p>in</p> <p>sprejeti so bili ukrepi za zmanjšanje tveganja, da identiteta pravne osebe ni enaka identiteti, ki se izkazuje, pri čemer so bila upoštevana na primer tveganja izgube, kraje, začasne razveljavitve, preklica ali izteka veljavnosti dokaza;</p> <p>ali</p> <p>2. kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.3 za srednjo raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da tako enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ;</p> <p>ali</p> <p>3. kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašene sredstva elektronske identifikacije s srednjo ali visoko ravno zanesljivosti, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora srednjo in visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ.</p>
Visoka	<p>Poleg ravni „Srednja“ mora biti izpolnjena še ena izmed možnosti iz točk 1 do 3:</p> <p>1. identiteta pravne osebe, ki se izkazuje, je dokazana na podlagi dokaza, ki ga priznava država članica, v kateri je bila vložena vloga za sredstvo elektronske identifikacije, vključno z imenom pravne osebe, pravno obliko in najmanj enim enoličnim identifikatorjem, ki predstavlja pravno osebo, kot se uporablja v nacionalnem kontekstu;</p> <p>in</p> <p>preverja se veljavnost dokaza v skladu z verodostojnim virom;</p> <p>ali</p>

Raven zanesljivosti	Zahtevani elementi
	<p>2. kadar postopki, ki so jih predhodno uporabljali javni ali zasebni subjekti v isti državi članici za namen, ki ni izdajanje sredstev elektronske identifikacije, zagotavljajo enakovredno raven zanesljivosti, ki ustreza tistim v oddelku 2.1.3 za visoko raven zanesljivosti, subjektu, odgovornemu za registracijo, ni treba ponavljati navedenih predhodnih postopkov, pod pogojem, da tako enakovredno raven zanesljivosti potrjuje organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ;</p> <p>in</p> <p>sprejeti so bili ukrepi za dokazovanje, da so rezultati tega predhodnega postopka še vedno veljavni;</p> <p>ali</p> <p>3. kadar so sredstva elektronske identifikacije izdana na podlagi veljavnega priglašene sredstva elektronske identifikacije z visoko ravno zanesljivosti, se ne zahteva ponavljanje postopkov za dokazovanje in preverjanje identitete. Kadar sredstvo elektronske identifikacije, ki služi kot podlaga, ni bilo priglašeno, mora visoko raven zanesljivosti potrditi organ za ugotavljanje skladnosti iz člena 2(13) Uredbe (ES) št. 765/2008 ali enakovredni organ;</p> <p>in</p> <p>sprejeti so bili ukrepi za dokazovanje, da so rezultati predhodnega postopka za izdajo priglašene sredstva elektronske identifikacije še vedno veljavni.</p>

2.1.4 Povezava med sredstvi elektronske identifikacije fizičnih in pravnih oseb

Za povezavo med sredstvi elektronske identifikacije fizične osebe in sredstvi elektronske identifikacije pravne osebe (v nadaljnjem besedilu: povezava) se, kadar je to primerno, uporabljajo naslednji pogoji:

1. Povezavo je mogoče začasno razveljaviti in/ali preklicati. Življenjski cikel povezave (npr. aktiviranje, začasna razveljavitev, podaljšanje, preklic) se upravlja v skladu s priznanimi postopki na nacionalni ravni.
2. Fizična oseba, katere sredstvo elektronske identifikacije je povezano s sredstvom elektronske identifikacije pravne osebe, lahko izvajanje povezave prenese na drugo fizično osebo na podlagi priznanih postopkov na nacionalni ravni. Vendar pa je odgovornost še vedno na strani fizične osebe.
3. Povezava se izvede na naslednji način:

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Dokazovanje identitete fizične osebe, ki deluje v imenu pravne osebe, je preverjeno na ravni „Nizka“ ali višji. 2. Povezava je bila vzpostavljena na podlagi priznanih postopkov na nacionalni ravni. 3. Verodostojnemu viru ni znano, da bi bila fizična oseba v stanju, ki bi ji onemogočalo, da deluje kot navedena pravna oseba.
Srednja	<p>Poleg točke 3 ravni „Nizka“ še:</p> <ol style="list-style-type: none"> 1. Dokazovanje identitete fizične osebe, ki deluje v imenu pravne osebe, je preverjeno na ravni „Srednja“ ali „Visoka“.

Raven zanesljivosti	Zahtevani elementi
	<ol style="list-style-type: none"> 2. Povezava je bila vzpostavljena na podlagi priznanih postopkov na nacionalni ravni, posledica česar je bila registracija povezave v verodostojnem viru. 3. Povezava je bila preverjena na podlagi informacij iz verodostojnega vira.
Visoka	<p>Poleg točke 3 ravni „Nizka“ in točke 2 ravni „Srednja“ še:</p> <ol style="list-style-type: none"> 1. Dokazovanje identitete fizične osebe, ki deluje v imenu pravne osebe, je bilo preverjeno na ravni „Visoka“. 2. Povezava je bila preverjena na podlagi enoličnega identifikatorja, ki predstavlja pravno osebo, ki se uporablja v nacionalnem okviru, in na podlagi informacij iz verodostojnega vira, ki enolično predstavljajo fizično osebo.

2.2 Upravljanje sredstev elektronske identifikacije

2.2.1 Lastnosti in zasnova sredstev elektronske identifikacije

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Sredstvo elektronske identifikacije uporablja najmanj en dejavnik avtentikacije. 2. Sredstvo elektronske identifikacije je zasnovano tako, da izdajatelj sprejme razumne ukrepe, s katerimi preveri, da se uporablja le pod nadzorom ali v posesti osebe, ki ji pripada.
Srednja	<ol style="list-style-type: none"> 1. Sredstvo elektronske identifikacije uporablja najmanj dva dejavnika avtentikacije iz različnih kategorij. 2. Sredstvo elektronske identifikacije je zasnovano tako, da se lahko domneva, da se uporablja le, kadar je pod nadzorom ali v posesti osebe, ki ji pripada.
Visoka	<p>Poleg ravni „Srednja“ še:</p> <ol style="list-style-type: none"> 1. Sredstvo elektronske identifikacije varuje pred podvajanjem in nedovoljenim posegom ter napadalci z visokim potencialom za napad. 2. Sredstvo elektronske identifikacije je zasnovano tako, da ga lahko oseba, ki ji pripada, zanesljivo zavaruje pred uporabo drugih oseb.

2.2.2 Izdaja, dostava in aktiviranje

Raven zanesljivosti	Zahtevani elementi
Nizka	Po izdaji se sredstvo elektronske identifikacije dostavi na način, pri katerem je mogoče domnevati, da je doseglo le osebo, ki ji je namenjeno.
Srednja	Po izdaji se sredstvo elektronske identifikacije dostavi na način, pri katerem je mogoče domnevati, da je bilo dostavljeno v posest le osebi, ki ji pripada.
Visoka	V postopku aktiviranja se preverja, da je bilo sredstvo elektronske identifikacije dostavljeno v posest le osebi, ki ji pripada.

2.2.3 Začasna razveljavitev, preklic in ponovno aktiviranje

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Sredstvo elektronske identifikacije je mogoče pravočasno in učinkovito začasno razveljaviti in/ali preklicati. 2. Obstajajo ukrepi za preprečitev nezakonite začasne razveljavitve, preklica in/ali ponovnega aktiviranja. 3. Ponovno aktiviranje se izvede le, če so še vedno izpolnjene enake zahteve glede zanesljivosti kot pred začasno razveljavitvijo ali preklicem.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.2.4 Podaljšanje in zamenjava

Raven zanesljivosti	Zahtevani elementi
Nizka	Ob upoštevanju tveganj za spremembo identifikacijskih podatkov osebe morajo biti za podaljšanje ali zamenjavo izpolnjene enake zahteve glede zanesljivosti kot pri prvotnem dokazovanju in preverjanju identitete oz. morata temeljiti na veljavnem sredstvu elektronske identifikacije z enako ali višjo ravno zanesljivosti.
Srednja	Enako kot za raven „Nizka“.
Visoka	Poleg ravni „Nizka“ še: kadar podaljšanje ali zamenjava temelji na veljavnem sredstvu elektronske identifikacije, se podatki o identiteti preverjajo na podlagi verodostojnega vira.

2.3 Avtentikacija

Ta oddelek se osredotoča na grožnje, ki so povezane z uporabo mehanizma avtentikacije in navaja zahteve za vsako raven zanesljivosti. V tem oddelku se šteje, da so nadzorni ukrepi sorazmerni tveganjem za dano raven zanesljivosti.

2.3.1 Mehanizem avtentikacije

Naslednja preglednica za vsako raven zanesljivosti določa zahteve glede na mehanizem avtentikacije, prek katerega fizična ali pravna oseba uporablja sredstvo elektronske identifikacije za potrjevanje identitete zanašajoči se stranki.

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Identifikacijski podatki osebe se izdajo po zanesljivem preverjanju sredstva elektronske identifikacije in njegove veljavnosti. 2. Kadar so identifikacijski podatki osebe shranjeni kot del mehanizma avtentikacije, morajo biti zavarovani, da se zaščitijo pred izgubo in zlorabo, vključno z nespletno analizo. 3. V mehanizmu avtentikacije se izvajajo varnostni nadzori za preverjanje sredstva elektronske identifikacije, zato je zelo malo verjetno, da bi napadalci z povečanim osnovnim potencialom za napad lahko z dejavnostmi, kot so ugibanje, prisluškovanje, ponovno predvajanje ali manipulacija s sporočilom, ogrozili mehanizme avtentikacije.

Raven zanesljivosti	Zahtevani elementi
Srednja	<p>Poleg ravni „Nizka“ še:</p> <ol style="list-style-type: none"> 1. Identifikacijski podatki osebe se izdajo po zanesljivem preverjanju sredstva elektronske identifikacije in njegove veljavnosti z dinamično avtentikacijo. 2. V mehanizmu avtentikacije se izvajajo varnostni nadzori za preverjanje sredstva elektronske identifikacije, zato je zelo malo verjetno, da bi napadalci z zmernim potencialom za napad lahko z dejavnostmi, kot so ugibanje, prisluškovanje, ponovno predvajanje ali manipulacija s sporočilom, ogrozili mehanizme avtentikacije.
Visoka	<p>Poleg ravni „Srednja“ še:</p> <p>v mehanizmu avtentikacije se izvajajo varnostni nadzori za preverjanje sredstva elektronske identifikacije, zato je zelo malo verjetno, da bi napadalci z visokim potencialom za napad lahko z dejavnostmi, kot so ugibanje, prisluškovanje, ponovno predvajanje ali manipulacija s sporočilom, ogrozili mehanizme avtentikacije.</p>

2.4 Upravljanje in organizacija

Vsi udeleženci, ki zagotavljajo čezmejne storitve v zvezi z elektronsko identifikacijo (v nadaljnjem besedilu: ponudniki) imajo dokumentirane postopke za upravljanje informacijske varnosti, politike, pristope za upravljanje tveganj in druge priznane nadzorne ukrepe, s katerimi se ustreznim organom upravljanja shem elektronske identifikacije v zadevnih državah članicah zagotavlja, da so vzpostavljeni učinkoviti postopki. V oddelku 2.4. se šteje, da so vse zahteve/elementi sorazmerni tveganjem za dano raven zanesljivosti.

2.4.1 Splošne določbe

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Ponudniki katerih koli operativnih storitev iz te uredbe so javni organ ali pravni subjekt, ki ga kot takega priznava nacionalno pravo države članice in ima vzpostavljeno organizacijo ter je polno operativen v vseh delih, ki so bistveni za opravljanje storitev. 2. Ponudniki izpolnjujejo vse pravne zahteve, ki so jim naložene v zvezi z izvajanjem in zagotavljanjem storitve, vključno s tem, katere vrste informacij se lahko zahtevajo, kako se izvaja dokazovanje identitete, katere informacije se lahko hranijo in kako dolgo. 3. Ponudniki lahko dokažejo, da so sposobni prevzeti škodno odgovornost in da imajo zadostne finančne vire za neprekinjeno delovanje in zagotavljanje storitev. 4. Ponudniki so odgovorni za izpolnjevanje vseh zavez, ki jih prenesejo na zunanje izvajalce, in skladnost s politiko sheme v enaki meri, kot če bi naloge opravili sami. 5. Za sheme elektronske identifikacije, ki niso bile vzpostavljene na podlagi nacionalne zakonodaje, je pripravljen učinkovit načrt prenehanja delovanja. Tak načrt mora vključevati urejeno prekinitev storitve ali nadaljevanje izvajanja prek drugega ponudnika, način obveščanja zadevnih organov in končnih uporabnikov ter podrobnosti o načinu zavarovanja, hrambe in uničenja podatkov v skladu s politiko sheme.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.2 Objavljena obvestila in uporabniške informacije

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Obstaja objavljena opredelitev storitve, ki vključuje vse uporabljene izraze, pogoje in pristojbine, vključno z vsemi omejitvami uporabe. Opredelitev storitve vključuje tudi politiko varstva osebnih podatkov. 2. Vzpostaviti je treba ustrezno politiko in postopke, da se zagotovi pravočasna in zanesljiva obveščena uporabnikov storitve o vseh spremembah opredelitve storitve in uporabljenih izrazov, pogojev ter politike varstva zasebnosti za zadevno storitev. 3. Vzpostaviti je treba ustrezne politike in postopke, ki zagotavljajo celovite in pravilne odgovore na zahteve za informacije.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.3 Upravljanje informacijske varnosti

Raven zanesljivosti	Zahtevani elementi
Nizka	Obstaja učinkovit sistem upravljanja informacijske varnosti za upravljanje in nadzor tveganj v zvezi z informacijsko varnostjo.
Srednja	Poleg ravni „Nizka“ še: sistem za upravljanje informacijske varnosti upošteva dokazane standarde ali načela za upravljanje in nadzor tveganj v zvezi z informacijsko varnostjo.
Visoka	Enako kot za raven „Srednja“.

2.4.4 Vodenje evidence

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Vodenje evidence in hramba zadevnih informacij z uporabo učinkovitega sistema za upravljanje evidence ob upoštevanju veljavne zakonodaje in dobrih praks v zvezi z varstvom in hrambo podatkov. 2. Evidence se v dovoljenem obsegu v skladu z nacionalnim pravom ali drugo nacionalno upravno ureditvijo hranijo in varujejo tako dolgo, dokler se potrebujejo za revizijo in preiskovanje kršitev varnosti ter hrambo podatkov, nato se evidence varno uničijo.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.5 Prostor in osebje

Naslednja preglednica vsebuje zahteve v zvezi s prostori, osebjem in, kadar je to primerno, podizvajalci, ki izvajajo naloge iz te uredbe. Skladnost z vsako od zahtev je sorazmerna tveganju, ki je povezano z zagotovljeno ravno zanesljivosti.

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Obstajajo postopki, s katerimi se zagotavlja, da so osebe in podizvajalci za naloge, ki jih izvajajo, dovolj usposobljeni, kvalificirani in izkušeni. 2. Na voljo je dovolj osebja in podizvajalcev za ustrezno izvajanje in financiranje storitve v skladu z njenimi politikami in postopki. 3. Prostori, ki se uporabljajo za zagotavljanje storitve, so pod stalnim nadzorom in zavarovani pred škodo, ki jo povzročajo okoljski dogodki, nepooblaščen dostop in drugi dejavniki, ki bi lahko vplivali na varnost storitve. 4. Prostori, ki se uporabljajo za zagotavljanje storitve, omogočajo, da je dostop do območij, kjer se nahajajo ali obdelujejo osebni, kriptografski ali drugi občutljivi podatki, dovoljen le pooblaščenemu osebju ali podizvajalcem.
Srednja	Enako kot za raven „Nizka“.
Visoka	Enako kot za raven „Nizka“.

2.4.6 Tehnični nadzor

Raven zanesljivosti	Zahtevani elementi
Nizka	<ol style="list-style-type: none"> 1. Obstaja sorazmeren tehnični nadzor za upravljanje tveganj v zvezi z varnostjo storitev, ki varujejo zaupnost, celovitost in razpoložljivost obdelanih informacij. 2. Elektronski komunikacijski kanali, ki se uporabljajo za izmenjavo osebnih ali občutljivih podatkov, so zavarovani pred prisluškovanjem, manipulacijo in ponovnim predvajanjem. 3. Če se občutljivi kriptografski material uporablja za izdajo sredstva elektronske identifikacije in avtentikacijo, je dostop do njega omejen na uporabniške vloge in aplikacije, ki nujno potrebujejo dostop. Zagotavlja se, da se tak material nikoli ne hrani v golem besedilu. 4. Obstajajo postopki, ki zagotavljajo trajnostno vzdrževanje varnosti in zmožnost odgovora na spremembe ravni tveganja, incidente in kršitve varnosti. 5. Vsi mediji, ki vsebujejo osebne, kriptografske ali druge občutljive podatke, se shranjujejo, prevažajo in odstranjujejo na varen in zanesljiv način.
Srednja	<p>Poleg ravni „Nizka“ še:</p> <p>če se občutljiv kriptografski material uporablja za izdajo sredstev elektronske identifikacije in avtentikacijo, je zavarovan pred nedovoljenim posegom.</p>
Visoka	Enako kot za raven „Srednja“.

2.4.7 Skladnost in revizija

Raven zanesljivosti	Zahtevani elementi
Nizka	Obstajajo redne notranje revizije, ki zajamejo vse ustrezne dele za izvajanje zagotovljenih storitev, da se zagotovi skladnost z zadevno politiko.

Raven zanesljivosti	Zahtevani elementi
Srednja	Obstajajo redne neodvisne notranje ali zunanje revizije, ki zajamejo vse ustrezne dele za izvajanje zagotovljenih storitev, da se zagotovi skladnost z zadevno politiko.
Visoka	<ol style="list-style-type: none"><li data-bbox="448 338 1418 414">1. Obstajajo redne neodvisne zunanje revizije, ki zajamejo vse ustrezne dele za izvajanje zagotovljenih storitev, da se zagotovi skladnost z zadevno politiko.<li data-bbox="448 414 1418 492">2. Kadar shemo neposredno upravlja vladni organ, se revizija izvaja v skladu z nacionalno zakonodajo.