IDENTITETA JE ZAUPANJE. ZAUPANJE JE PRIHODNOST.

INŠTITUT 1. APRIL

STRATEŠKA POBUDA

ZA VZPOSTAVITEV NAPREDNEGA BIOMETRIČNEGA SISTEMA
ZA ZAŠČITO OTROK (QEI)



ZA VARNOST. ZA PRAVICO. ZA PRIHODNOST.

ZA LJUDI. ZA DRUŽBO. ZA SVET.

Inštitut 1.april®

RAZISKAVE • INOVACIJE • NAPREDNE TEHNOLOGIJE

IZOLA, SLOVENIJA | institut1april.com | 2026

QEI INICIATIVA

IDENTITETA PRIHODNOSTI.
ZA LJUDI. ZA DRUŽBO. ZA SVET.

Quantized Encrypted Identity (QEI) je napreden, prostovoljen in varen sistem digitalne identitete, ki združuje **biometrijo, kriptografijo** in tehnologijo **decentraliziranih identitet** za **zaščito najbolj ranljivih** in podporo boljši prihodnosti za vse.

ZAŠČITA OTROK
Iskanje pogrešanih otrok, zaščita otrok brez spremstva in preprečevanje trgovine z otroki.

BEGUNCI IN MIGRANTI
Varna identiteta za begunce, migrante in druge ranljive skupine z dostojanstvom in zasebnostjo.

HUMANITARNA POMOČ
Učinkovita in pravična distribucija pomoči ter podpora humanitarnim organizacijam na terenu.

DIGITALNA IDENTITETA
Napredna digitalna identiteta brez gesel, brez surove biometrije in brez centraliziranih baz občutljivih podatkov.



VARNOST IN ZASEBNOST
Lokalna obdelava v varnih okoljih (TEE / Secure Enclave) in kriptografska zaščita najvišjega razreda.

ČLOVEKOVE PRAVICE
Spoštovanje dostojanstva, pravice do zasebnosti in načela minimalizacije podatkov.

GLOBALNA UPORABA
Interoperabilnost z evropskimi in mednarodnimi standardi (eIDAS 2.0, GDPR) za uporabo po vsem svetu.

PARTNERSTVO
Skupaj gradimo svet, v katerem je varna identiteta pravica – ne privilegij.

QEI – TEHNOLOGIJA, KI ZDRUŽUJE

VEČFAKTORSKA BIOMETRIJA
Združuje več biometričnih faktorjev za visoko stopnjo zaupanja in natančnosti.

KRIPTOGRAFSKA ZAŠČITA
Napredni kriptografski algoritmi za nepovratno transformacijo identitete.

LOKALNA OBDELAVA
Biometrija nikoli ne zapusti naprave. Zasebnost je vgrajena v sistem.

DECENTRALIZIRANA IDENTITETA
Uporabnik je lastnik svoje identitete. Brez centralnih baz in brez odvisnosti.

REGENERACIJA IDENTITETE
Možnost preklica in ustvarjanja nove identitete brez bioloških sprememb.

SKLADNOST IN ETIKA
Skladnost z GDPR, eIDAS 2.0 in najvišjimi etičnimi standardi.

NAŠA ZAVEZA

DOSTOJANSTVO – Vsaka oseba si zasluži spoštovanje.

SOLIDARNOST – Tehnologija v službi človeka.

PRAVIČNOST – Enake možnosti za vse.

INOVATIVNOST – Napredne rešitve za boljši svet.

TRAJNOST – Za prihodnje generacije in naš planet.

SKUPAJ USTVARJAMO SVET, V KATEREM JE IDENTITETA **VARNA, ZASEBNA** IN **DOSTOPNA VSEM.**

Inštitut 1.april™

RAZISKAVE • INOVACIJE • NAPREDNE TEHNOLOGIJE

K A Z A L O

0. STRATEŠKI RAZLOG ZA UKREPANJE (ZAKAJ ZDAJ) stran **8**
0.1 POENOSTAVLJEN PRIKAZ DELOVANJA SISTEMA 9

1. UVOD **9**

2. IZHODIŠČE IN NAMEN POBUDE **10**
2.1 Izhodišče 10
2.2 Namen pobude 10

3. TEMELJNA NAČELA SISTEMA **11**
3.1 Načelo prostovoljnosti 11
3.2 Načelo namenske omejitve 11
3.3 Načelo minimalizacije podatkov 11
3.4 Načelo nepovratne tokenizacije 11
3.5 Načelo ločenosti evidenc 12
3.6 Načelo sodnega in neodvisnega nadzora 12

4. PRAVNI IN ETIČNI OKVIR **12**
4.1 Ustavni okvir 12
4.2 Evropski pravni okvir 12
4.3 Etična izhodišča 12
4.4 Test sorazmernosti 13
4.5 Pravni test sorazmernosti 13
4.5.1 Legitimen cilj 13
4.5.2 Nujnost ukrepa 13
4.5.3 Minimalni poseg 13
4.5.4 Sorazmernost v ožjem smislu 13
4.6 Pravna definicija uporabe transformiranega STR vzorca 14
4.7 Izrecna prepoved zlorab 14
4.8 Ključno načelo ločitve identitete 15
4.9 Pravna pojasnitev: razbijanje mitov o biometričnih sistemih 15
4.9.1 GDPR ne prepoveduje, temveč strogo regulira 15
4.9.2 Ključna razlika: sistem ne uporablja DNK kot podatka 15
4.9.3 Skladnost z načelom *privacy by design* 16
4.9.4 Ustavna podlaga: zaščita otrok kot nadrejena vrednota 16
4.9.5 Sistem kot izjemni zaščitni mehanizem, ne nadzorni sistem 16
4.9.6 Zaključek pravne razjasnitve 16

5. MOŽNI MODEL IZVEDBE **17**
5.1 Osnovni izvedbeni model 17
5.2 Institucionalni okvir 17
5.3 Dopolnilna narava sistema 17
5.4 Upravljanje in nosilec sistema 17

6. PROSTOVOLJNI MODEL VKLJUČITVE **18**
6.1 Prostovoljna vključitev odraslih 18
6.2 Prostovoljna vključitev otrok 18
6.3 Prostovoljna možnost ob rojstvu 18

7. QEI - BIOMETRIČNI IDENTIFIKACIJSKI TOKEN stran **18**
7.1 Opredelitev 18
7.2 Ključne značilnosti 19
7.3 Česa QEI ne sme vsebovati 19
7.4 Pravna definicija sistema QEI 19
7.5 QEI - Physical Emergency Trigger Suite (PET-S) 19
7.5.1 Skupna logika (enoten sistem) 20
7.5.2 PET-1: QEI fizični ključek 20
7.5.3 PET-2: Emergency kartica (Child ID) 21
7.5.4 PET-3: Panic Trigger (naprava) 22
7.5.5 Integracija v sistem 24

8. PREDLOG ARHITEKTURE IN PODATKOVNEGA MODELA QEI SISTEMA **24**
8.1 Osnovna arhitektura 24
8.2 Ločene evidence 25
8.3 Načelo delovanja sistema 25
8.4 Pravno definirana arhitektura sistema 26

9. TRILOCK - TRIFAKTORSKI VARNOSTNI MODEL **26**
9.1 Osnovna zasnova 26
9.2 Pragovni model uporabe 26
9.3 Združevanje ključev 27
9.4 Ključna prednost modela 27
9.5 Način delovanja ključnega mehanizma QEI 27
9.6 QEI ONE - enotni varnostni ključ 28

10. STR-BIOMETRIČNI VZOREC KOT DODATNI FAKTOR **30**
10.1 Pravilna vloga STR komponente 30
10.2 Proces obdelave 30
10.3 Temeljna pravila 30
10.4 Pravna prednost takšne zasnove 31

11. KRIPTOGRAFSKA AVTENTIKACIJA **31**
11.1 Načelo *challenge-response* 31
11.2 Česa sistem nikoli ne pošilja 31
11.3 Načelo *fail-safe* 31

12. LOKALNA OBDELAVA IN VARNI MODULI **32**
12.1 Lokalna obdelava 32
12.2 Prepoved iznosa biometrije 32
12.3 Lokalna hramba ključev 32
12.4 Brez centralne baze biometrije 32

13. OBVEŠČANJE UPORABNIKA IN NADZOR UPORABE **32**
13.1 Načelo transparentnosti uporabe 32
13.2 Obvestilo uporabniku 33
13.3 Revizija in odgovornost 33

14. REVOCATION IN UPRAVLJANJE ŽIVLJENJSKEGA CIKLA IDENTITETE stran **33**
14.1 Revocation 33
14.2 Prednost 33
14.3 Upravljanje idenitete brez spremembe bioloških lastnosti 34

15. NORMATIVNE ZAHTEVE **34**
15.1 Dodatne normativne zahteve 34

16. VARNOSTNE IN PRAVNE VAROVALKE **35**

17. FINANČNI IN RAZVOJNI OKVIR **35**
17.1 Možni viri financiranja 35
17.2 Okvirna ocena stroškov 35
17.3 Intelektualna lastnina in patentna zaščita 35

18. JAVNA PREDSTAVITEV IN OBVEŠČANJE JAVNOSTI **36**

19. PREDLOG NADALJNJIH KORAKOV **37**
19.1 Strateška usmeritev nadaljnjih korakov 37
19.2 Predlog pilotnega projekta 38

20. URADNI PREDLOG ZA VLADO REPUBLIKE SLOVENIJE **38**

21. PRAVNI ARGUMENTI ZA NADALJNJO STROKOVNO RAZPRAVO **39**
21.1 Razširjeni pravni argumenti 39

22. INDIKATIVNI STATISTIČNI PREGLED IN DODATKI **39**
22.1 Indikativni statistični pregled 39
22.2 Ugrabitve oziroma odtujitve novorojenčkov iz porodnišnic 41
22.3 Globalna trgovina z ljudmi - delež otrok 41
22.4 Viri za spremno gradivo / opombe 42

23. SKLEP **44**

24. VIRI IN LITERATURA **45**
24.1 Mednarodni pravni akti 45
24.2 Evropska zakonodaja 45
24.3 Nacionalna zakonodaja Republike Slovenije 45
24.4 Mednarodni standardi in strokovne smernice 45
24.5 Strokovna literatura 46

25. SLOVAR KLJUČNIH POJMOV, KRATIC IN TUJK **47**

PRILOGA I - DODATNA STROKOVNA DOPOLNITEV:
MANJKAJOČI KLJUČNI ELEMENTI ZA REALNO IZVEDBO **51**
I.1 Root of Trust 51
I.2 Pravna podlaga (GDPR + eIDAS + nacionalni okvir) 51
I.3 Upravljanje ključev (Key Management) 52
I.4 Standardi in interoperabilnost 52
I.5 Verifikacijski tok (Verification Flow) 53

I.6 Napadi in zlorabe stran 53
I.7 Realni scenariji uporabe 53
I.8 Financiranje in upravljanje 54

PRILOGA II - DODATNA VARNOSTNA DOPOLNITEV:
THREAT MODEL, VARNOSTNA ARHITEKTURA IN CERTIFIKACIJSKA USMERITEV 55
II.1 Osnovna varnostna premisa 55
II.2 Glavne površine napada 55
II.3 Tipični napadi in predlagane zaščite 55
II.4 Slojna varnostna arhitektura 57
II.5 Certifikacijska in standardizacijska usmeritev 57
II.6 Ključni zaključek varnostne dopolnitve 58

PRILOGA III - OPERATIVNI OKVIR ZA NADALJNJO OBRAVNAVO POBUDE 59
III.1 Priprava enotnega formalnega dokumenta 59
III.2 Pravna dopolnitev in validacija 59
III.3 Vsebinska koncentracija osrednjega namena 60
III.4 Določitev pristojnih naslovnikov 60
III.5 Predložitev pobude kot uradnega dokumenta 60
III.6 Zaključna operativna usmeritev 61

PRILOGA IV - SISTEM ZA HUMANITARNO IDENTITETO IN POMOČ QEI (QHIAS) 63
IV.1 Uvod 63
IV.2 Namen sistema 63
IV.3 Humanitarna digitalna identiteta 63
IV.4 Digitalna humanitarna denarnica 64
IV.5 Zaščita otrok brez spremstva 64
IV.6 Preprečevanje trgovine z ljudmi 65
IV.7 Pravne in etične varovalke 65
IV.8 Pametna distribucija pomoči 66
IV.9 Digitalna identiteta za osebe brez dokumentov 66
IV.10 Možna povezava z evropsko digitalno identiteto 66
IV.11 Pilotni projekt Evropske unije 67
IV.12 Sklep 67

PRILOGA V - TEHNIČNA ARHITEKTURA IN OKVIR PRIHODNJEGA RAZVOJA QEI 69
V.1 Namen priloge 69
V.2 Večfaktorski biometrični model 69
V.3 Stabilizacija biometričnih podatkov 70
V.4 Generiranje kriptografske identitete 71
V.5 Lokalna obdelava in varni moduli 71
V.6 Kriptografska avtentikacija 72
V.7 Decentralizirana digitalna identiteta 72
V.8 Možni produkti in področja uporabe 73
V.9 Upravljanje življenjskega cikla identitete 74
V.10 Varnostne prednosti arhitekture 75
V.11 Raziskovalni in razvojni potencial 75
V.12 Zaključek 76



POVZETEK

Inštitut 1. april predstavlja strateško pobudo za razvoj naprednega sistema digitalne identitete, namenjenega zaščiti otrok in drugih posebej ranljivih skupin.

Predlagana rešitev uvaja biometrični identifikacijski sistem **QEI (Quantized Encrypted Identity)**, ki temelji na anonimiziranih in nepovratno transformiranih biometričnih podatkih. Sistem ne shranjuje bioloških vzorcev, genetskih zapisov ali surovih biometričnih podatkov, temveč ustvarja kriptografske identifikacijske žetone (tokene), ki omogočajo varno preverjanje identitete izključno na podlagi ustrezne pravne podlage in pod strogim nadzorom.

Rešitev je zasnovana v skladu z načeli **privacy by design**, minimizacije podatkov, omejitve namena obdelave ter ločenosti evidenc in je skladna z evropskim pravnim okvirom, vključno s **Splošno uredbo o varstvu podatkov (GDPR)**, **Listino Evropske unije o temeljnih pravicah** ter drugimi relevantnimi standardi za varstvo osebnih podatkov.

Sistem lahko pomembno prispeva k iskanju pogrešanih otrok, preprečevanju trgovine z ljudmi, odkrivanju nezakonitih posvojitev ter reševanju primerov, v katerih identifikacija z obstoječimi metodami ni mogoča ali ni dovolj zanesljiva.

Predlagana rešitev temelji na izvirnih tehnoloških konceptih s področij biometrije, kriptografije in digitalne identitete, za katere potekajo postopki zaščite intelektualne lastnine in patentnega varstva.

Ustanovitev **Inštituta 1. april** ter nadaljnji razvoj sistema **QEI** predstavljata pomemben korak k vzpostavitvi varne, etične, tehnološko napredne in zasebnost varujoče digitalne identitete prihodnosti v Republiki Sloveniji, Evropski uniji in širši mednarodni skupnosti.

e: info@institut1april.com
w: institut1april.com

POBUDA ZA JAVNO RAZPRAVO IN PRIPRAVO ZAKONODAJE

BIOMETRIČNI IDENTIFIKACIJSKI SISTEM ZA ZAŠČITO OTROK (QEI)

Predlagatelj:

Inštitut 1. april
e: info@institut1april.com
w: institut1april.com

Verzija 1.0 - April 2026

0. STRATEŠKI RAZLOG ZA UKREPANJE (ZAKAJ ZDAJ)

V zadnjih letih se Evropska unija in države članice soočajo z naraščajočimi izzivi na področju zaščite otrok, zlasti v kontekstu:

- čezmejnih migracij,
- organiziranega kriminala in trgovine z ljudmi,
- nezakonitih posvojitev,
- digitalnih zlorab identitete,
- razvoja umetne inteligence in tehnologij *deepfake*.

Obstoječi identifikacijski sistemi temeljijo predvsem na administrativnih evidencah, ki niso neposredno povezane z biološko identiteto posameznika, kar v izjemnih primerih omogoča manipulacijo ali zlorabo identitete.

Hkrati Evropska unija razvija nove okvire digitalne identitete (eIDAS 2.0), kar odpira možnost vključitve naprednih, zasebnostno varnih mehanizmov identifikacije.

Zato se postavlja ključno vprašanje:

Ali lahko država in Evropska unija razvijeta sistem, ki bi:

- izboljšal zaščito otrok,
- preprečil najtežje oblike zlorab,
- deloval brez centralne baze podatkov,
- spoštoval najvišje standarde varstva zasebnosti?

Ta pobuda predstavlja odgovor na to vprašanje in predlaga, da se takšen sistem vsaj strokovno, pravno in tehnično preuči.

0.1 POENOSTAVLJEN PRIKAZ DELOVANJA SISTEMA

Za lažje razumevanje je osnovno delovanje sistema mogoče povzeti v štirih korakih:

1. Otrok (in starši) se prostovoljno vključijo v sistem.
2. Iz minimalnih biometričnih vhodov se ustvari anonimiziran kriptografski token.
3. V primeru incidenta se preveri ujemanje med tokeni.
4. Identiteta se lahko razkrije izključno na podlagi pravne podlage in ustreznega nadzora.

Sistem:

- ne hrani surovih biometričnih podatkov,
- ne vsebuje centralne baze identitet,
- ne omogoča splošnega nadzora,
- deluje izključno v izjemnih primerih.

1. UVOD

Ta pobuda predlaga začetek strokovne in javne razprave o možnosti uvedbe prostovoljnega biometričnega identifikacijskega sistema za zaščito otrok, ki temelji na uporabi anonimiziranih kriptografskih identifikacijskih tokenov (QEI).

Izključni namen predlaganega sistema bi bil:

- iskanje pogrešanih otrok,
- preprečevanje trgovine z otroki,
- razkrivanje nezakonitih posvojitev,
- preverjanje biološkega sorodstva v primerih utemeljenega suma hudih kaznivih dejanj nad otroki.

Namen pobude je preučiti možnost vzpostavitve pravno strogo omejenega, tehnično varnega in ustavno sorazmernega sistema, ki bi deloval izključno v interesu zaščite otrok ob polnem spoštovanju:

- Ustave Republike Slovenije,
- prava Evropske unije,
- pravil o varstvu osebnih podatkov,
- načela sorazmernosti,
- načela najmanjšega možnega posega v pravice posameznika.

Kljub obstoječim sistemom evidentiranja rojstev in identifikacije oseb še vedno obstajajo primeri, v katerih identiteta otroka ni zanesljivo preverljiva ali je bila nezakonito spremenjena. Takšne vrzeli lahko predstavljajo resno tveganje za zaščito otrok, zlasti v primerih:

- trgovine z ljudmi,
- nezakonitih posvojitev,
- čezmejnih kaznivih dejanj,
- sporov glede starševstva,
- pogrešanih otrok brez možnosti zanesljive identifikacije.

Obstoječi sistemi praviloma temeljijo na administrativnih evidencah, ki niso neposredno povezane z biološko identiteto. Predlagani sistem QEI odpira razpravo o možnosti preverjanja identitete na podlagi minimalnih, anonimiziranih in nepovratno obdelanih biometričnih vhodov brez shranjevanja surovih ali bioloških podatkov.

Biometrični podatki v sistemu ne predstavljajo identitete, temveč bi služili izključno kot lokalni mehanizem za odklep kriptografskega ključa oziroma za generiranje nepovratnega identifikacijskega tokena v strogo omejenih postopkih.

Nedavni čezmejni primeri trgovine z otroki, manipulacij identitete, nezakonitih posvojitev ter povečana tveganja digitalnih zlorab kažejo na potrebo po razmisleku o novih, zasebnostno varnih mehanizmih za zaščito otrok. Namen te pobude je proaktivno odpreti strokovno in javno razpravo o možnih rešitvah, še preden se takšna tveganja dodatno povečajo.

Zaradi čezmejne narave trgovine z otroki, nezakonitih posvojitev in primerov pogrešanih otrok ima pobuda potencialno razsežnost tudi na ravni Evropske unije. Morebitni nadaljnji razvoj bi zato lahko v prihodnje preučil tudi interoperabilnost z evropskimi okviri ob strogem spoštovanju pravil varstva osebnih podatkov, načela subsidiarnosti in ustavnih omejitev.

Tehnični model, predstavljen v nadaljevanju, je podan na konceptualni ravni z namenom prikaza izvedljivosti, varnostnih načel in pravnih varovalk. Podrobna implementacija bi bila predmet nadaljnje strokovne, tehnične in pravne analize.

Če obstaja tehnologija, ki lahko reši življenje enega pogrešanega otroka, je dolžnost države, da vsaj preveri njeno ustavno, pravno in tehnično izvedljivost.

2. IZHODIŠČE IN NAMEN POBUDE

2.1 Izhodišče

Pobuda izhaja iz potrebe po razpravi o dodatnem zaščitnem mehanizmu za otroke, zlasti v primerih:

- trgovine z otroki,
- suženjstva in spolnega izkoriščanja otrok,
- kraje otrok ob rojstvu,
- nezakonitih oziroma ilegalnih posvojitev,
- sistemskih napak pri evidentiranju starševstva,
- primerov pogrešanih otrok brez zanesljive identifikacije.

Čeprav so takšni primeri statistično razmeroma redki, gre za izredno občutljiva in težka kazniva dejanja, pri katerih lahko že posamezen primer predstavlja izjemno hud poseg v človekove pravice in dostojanstvo otroka.

2.2 Namen pobude

Namen pobude je odpreti strokovno, pravno, tehnično in etično razpravo o možnosti vzpostavitve sistema, ki bi:

- deloval izključno za zaščito otrok,
- bil prostovoljen,
- uporabljal minimalne biometrične predloge,
- ne bi shranjeval bioloških vzorcev ali surovih biometričnih podatkov,
- omogočal uporabo le ob strogi pravni podlagi,
- bil podvržen neodvisnemu nadzoru,
- preprečeval vsakršno širitev namena uporabe.

3. TEMELJNA NAČELA SISTEMA

Predlagani sistem bi moral temeljiti na naslednjih načelih.

3.1 Načelo prostovoljnosti

Vključitev v sistem bi bila mogoča izključno na podlagi svobodne, informirane in izrecne privolitve.

3.2 Načelo namenske omejitve

Sistem bi se smel uporabljati izključno za zaščito otrok, zlasti za:

- iskanje pogrešanih otrok,
- preprečevanje trgovine z otroki,
- razkrivanje nezakonitih posvojitev,
- preverjanje biološkega sorodstva v primerih zakonsko dopustnega postopka.

Uporaba za druge namene bi morala biti izrecno prepovedana, zlasti za:

- splošni kazenski pregon odraslih,
- davčne postopke,
- zdravstvene analize,
- komercialne namene,
- splošni nadzor prebivalstva.

3.3 Načelo minimalizacije podatkov

Sistem ne bi smel hraniti:

- bioloških vzorcev po obdelavi,
- surovih biometričnih podatkov,
- celotnega genetskega zapisa,
- zdravstvenih genetskih podatkov,
- osebnih podatkov znotraj samega QEI tokena.

3.4 Načelo nepovratne tokenizacije

Sistem bi uporabljal izključno standardizirane biometrične predloge in iz njih ustvarjal nepovratne kriptografske identifikacijske tokene.

3.5 Načelo ločenosti evidenc

Identitetni podatki, biometrične predloge in revizijski podatki bi morali biti hranjeni strogo ločeno, brez enotne centralne baze občutljivih podatkov.

3.6 Načelo sodnega in neodvisnega nadzora

Dostop do podatkov oziroma sprožitev postopka identifikacije bi moral biti mogoč le na podlagi:

- zakonske podlage,
- sodne odredbe, kadar je ta zahtevana,
- stroge revizijske sledljivosti,
- neodvisnega institucionalnega nadzora.

4. PRAVNI IN ETIČNI OKVIR

Predlagani sistem bi moral biti zasnovan v skladu z naslednjimi pravnimi in etičnimi izhodišči.

4.1 Ustavni okvir

35. člen Ustave Republike Slovenije - varstvo pravice do zasebnosti in osebnostnih pravic,
36. člen Ustave Republike Slovenije - posebno varstvo otrok.

4.2 Evropski pravni okvir

- Splošna uredba o varstvu podatkov (**GDPR**), zlasti 6. in 9. člen,
- Listina Evropske unije o temeljnih pravicah - 7. in 8. člen,
- Evropska konvencija o človekovih pravicah - 8. člen.

4.3 Etična izhodišča

Predlagani sistem bi moral slediti naslednjim načelom:

- ***privacy by design***,
- ***privacy by default***,
- sorazmernosti,
- nujnosti,
- minimalnega posega,
- sledljivosti,
- odgovornosti,
- nepovezljivosti med sistemi,
- prepovedi sekundarne uporabe podatkov.

4.4 Test sorazmernosti

Vsaka morebitna zakonodajna ureditev bi morala prestati test sorazmernosti, ki vključuje:

- legitimen cilj - zaščito otrok,
- primernost ukrepa,
- nujnost ukrepa,
- najmanjši možni poseg v pravice posameznika.

4.5 Pravni test sorazmernosti

Predlagani sistem je zasnovan tako, da prestane test sorazmernosti v skladu z ustavno in evropsko sodno prakso.

4.5.1 Legitimen cilj

Zaščita otrok pred hudimi oblikami kaznivih dejanj predstavlja ustavno varovano vrednoto v smislu **56. člena Ustave Republike Slovenije** ter legitimen cilj v smislu **prava Evropske unij**e in **Evropske konvencije o človekovih pravicah**.

4.5.2 Nujnost ukrepa

Obstoječi administrativni sistemi ne omogočajo vedno zanesljive identifikacije v primerih:

- nezakonitih posvojitev,
- trgovine z otroki,
- čezmejnih primerov brez ustrezne dokumentacije,
- sporov glede starševstva v posebej občutljivih okoliščinah.

Predlagani sistem predstavlja dopolnilni mehanizem za izjemne primere, kjer milejši ukrepi ne zagotavljajo enake učinkovitosti.

4.5.3 Minimalni poseg

Sistem je zasnovan tako, da:

- ne shranjuje biometričnih ali genetskih podatkov v surovi obliki,
- uporablja zgolj transformirane, standardizirane in nereverzibilne predloge,
- deluje brez neposredne identifikacije posameznika,
- ne omogoča splošnega nadzora prebivalstva,
- identiteto razkrije le pod strogo določenimi pravnimi pogoji.

4.5.4 Sorazmernost v ožjem smislu

Predlagani ukrepi so strogo omejeni:

- na zaščito otrok,
- na prostovoljno vključitev,

- na sodni oziroma zakonsko določen nadzor,
- na izjemne in posebej občutljive primere.

Zaradi teh omejitev je poseg bistveno ožji od klasičnih centraliziranih sistemov obdelave biometričnih podatkov.

4.6 Pravna definicija uporabe transformiranega STR vzorca

V sistemu se DNK ne uporablja kot identifikacijski ali analitični podatek, temveč izključno kot transformiran, nereverzibilen biometrični vzorec, ki:

- ne omogoča neposredne identifikacije posameznika,
- ne vsebuje zdravstvenih ali dednih informacij,
- se uporablja izključno kot dodatni varnostni faktor za visoko stopnjo zaupanja.

Pri tem velja:

- surovi DNK podatki se nikoli ne shranjujejo,
- biološki vzorec se po obdelavi takoj in nepovratno uniči,
- iz transformiranega zapisa ni mogoče rekonstruirati izvornega DNK.

Transformirani STR vzorec se:

- ne uporablja za kontinuirano avtentikacijo,
- ne uporablja kot primarni identifikator,
- ne uporablja za zdravstvene, diagnostične ali raziskovalne namene.

Sistem ne uporablja DNK za identifikacijske namene v klasičnem pomenu, temveč izključno transformiran, nereverzibilen kriptografski faktor, ki ne omogoča razkritja genetskih ali zdravstvenih informacij.

4.7 Izrecna prepoved zlorab

Sistem se ne sme uporabljati za:

- splošni nadzor prebivalstva,
- kazenski pregon odraslih oseb zunaj strogo določenega področja zaščite otrok,
- davčne ali upravne postopke,
- zdravstvene analize,
- genetske raziskave,
- komercialne namene,
- profiliranje,
- avtomatizirano odločanje,
- množični nadzor ali sekundarno uporabo podatkov.

Vsaka razširitev namena uporabe, ki bi presegala izključno zaščito otrok v zakonsko določenih primerih, mora biti izrecno prepovedana in kazniva.

4.8 Ključno načelo ločitve identitete

Sistem sam po sebi ne omogoča identifikacije posameznika. Identifikacija je mogoča izključno:

- ob potrjenem ujemanju tokena ali drugega kriptografskega rezultata,
- ob izpolnjenih pravnih pogojih,
- na podlagi sodne odredbe ali druge zakonsko določene pravne podlage,
- ob evidentiranju dostopa v revizijski evidenci.

Brez izpolnitve navedenih pogojev identiteta ni dostopna.

4.9 Pravna pojasnitev: razbijanje mitov o biometričnih sistemih

V javnem prostoru pogosto obstaja napačno prepričanje, da evropski pravni okvir, zlasti Splošna uredba o varstvu podatkov (GDPR), v celoti prepoveduje uporabo biometričnih in genetskih podatkov. Takšna razlaga ni pravilna.

4.9.1 GDPR ne prepoveduje, temveč strogo regulira

GDPR v 9. členu določa, da so biometrični in genetski podatki posebna kategorija osebnih podatkov, katerih obdelava je načeloma omejena, vendar ni absolutno prepovedana.

Obdelava je dopustna, kadar obstaja:

- izrecna privolitev posameznika,
- pomemben javni interes,
- ustrezna pravna podlaga,
- sorazmeren in nujen ukrep.

Predlagani sistem je zasnovan prav na teh temeljih:

- popolna prostovoljnost,
- stroga namenska omejitev,
- minimalizacija podatkov,
- uporaba izključno v izjemnih primerih zaščite otrok.

4.9.2 Ključna razlika: sistem ne uporablja DNK kot podatka

V nasprotju s klasičnimi biometričnimi ali forenzičnimi bazami predlagani model:

- ne shranjuje DNK,
- ne hrani bioloških vzorcev,
- ne omogoča rekonstrukcije genetskih podatkov,
- ne vsebuje zdravstvenih ali drugih občutljivih informacij.

DNK oziroma STR komponenta se uporablja izključno kot lokalni kriptografski vhod za generiranje nepovratnega ključa.

To pomeni, da sistem:

- ne ustvarja genetske baze,
- ne omogoča identifikacije brez pravne podlage,
- ne predstavlja trajnega biološkega identifikatorja.

4.9.3 Skladnost z načelom *privacy by design*

Predlagana arhitektura že v osnovi izpolnjuje ključne zahteve evropskega prava:

- obdelava podatkov izključno lokalno (TEE / Secure Enclave),
- ločene evidence brez centralne baze,
- nepovratna tokenizacija,
- prepoved sekundarne uporabe podatkov,
- popolna sledljivost dostopa.

Takšna zasnova predstavlja celo višji standard varstva podatkov, kot ga imajo številni obstoječi sistemi.

4.9.4 Ustavna podlaga: zaščita otrok kot nadrejena vrednota

Ustava Republike Slovenije v 56. členu določa posebno varstvo otrok. To pomeni, da država ni le upravičena, temveč tudi dolžna preučiti ukrepe, ki lahko izboljšajo zaščito otrok, če so ti:

- sorazmerni,
- nujni,
- ustavno skladni.

4.9.5 Sistem kot izjemni zaščitni mehanizem, ne nadzorni sistem

Pomembno je poudariti, da predlagani sistem:

- ni namenjen splošni identifikaciji prebivalstva,
- ni namenjen nadzoru ali sledenju,
- ni uporaben brez pravne podlage,
- deluje izključno v izjemnih, zakonsko določenih primerih.

Gre za specializiran zaščitni mehanizem za najtežje primere, kjer obstoječi sistemi ne zadoščajo.

4.9.6 Zaključek pravne razjasnitve

Trditev, da evropski pravni red takšen sistem v celoti prepoveduje, ne drži. Nasprotno, ob ustrezni zasnovi, varovalkah in pravni ureditvi je mogoče razviti rešitev, ki:

- spoštuje temeljne pravice,
- sledi načelom varstva podatkov,
- hkrati pa učinkovito prispeva k zaščiti otrok.

Zato pobuda ne predstavlja odstopanja od veljavnega pravnega reda, temveč poskus njegove nadgradnje v smeri večje zaščite najranljivejših.

5. MOŽNI MODEL IZVEDBE

5.1 Osnovni izvedbeni model

Predlagani model bi lahko temeljil na naslednjih elementih:

- prostovoljni oddaji biometričnih vhodov staršev in otrok,
- obdelavi zgolj minimalnih biometričnih predlog,
- ustvarjanju izključno kriptografskega identifikacijskega tokena,
- prepovedi shranjevanja bioloških ali surovih biometričnih podatkov,
- aktivaciji postopkov izključno na podlagi pravno dopustnega postopka,
- neodvisnem institucionalnem nadzoru,
- strogih sankcijah za zlorabo.

5.2 Institucionalni okvir

Možni institucionalni okvir bi lahko vključeval:

- **Ministrstvo za notranje zadeve** - upravljanje sistema,
- **Ministrstvo za zdravje** - izvedbo odvzema ob vključitvi,
- **Policijo in kriminalistično službo** - operativno uporabo v zakonsko določenih primerih,
- **Informacijskega pooblaščenca** - nadzor nad varstvom osebnih podatkov,
- **neodvisni nadzorni organ** - revizijo delovanja sistema,
- **sodišča** - odločanje o dopustnosti posega in dostopa.

5.3 Dopolnilna narava sistema

Predlagani sistem ne uvaja nove oblike splošne identifikacije, temveč predstavlja dodatni, strogo omejeni zaščitni mehanizem za izjemne primere, kjer obstoječi sistemi odpovejo.

Sistem ni zamišljen kot nadomestilo za obstoječe evidence, temveč kot dopolnilni zaščitni sloj, namenjen posebej občutljivim primerom zaščite otrok.

5.4 Upravljanje in nosilec sistema

Za operativno izvedbo sistema je ključno jasno določiti nosilca projekta in upravljavsko strukturo.

Možna osnovna struktura bi lahko bila:

- **vodilna institucija:** država (npr. Ministrstvo za notranje zadeve) ali evropski okvir,
- **strokovni nosilec in razvojni partner:** Inštitut 1. april,
- **tehnološki partnerji:** TBD (razvoj, varnost, infrastruktura),
- **nadzorni organ:** neodvisna institucija (npr. Informacijski pooblaščenec).

Takšna razdelitev omogoča:

- jasno odgovornost,
- institucionalno legitimnost,

- strokovno podporo,
- transparentnost upravljanja.

6. PROSTOVOLJNI MODEL VKLJUČITVE

6.1 Prostovoljna vključitev odraslih

Odrasli posameznik bi se lahko vključil v sistem na podlagi pisnega in informiranega soglasja.

Kadarkoli bi moral imeti pravico zahtevati izbris podatkov, če za njihovo hrambo ne obstaja druga zakonska podlaga.

6.2 Prostovoljna vključitev otrok

Vključitev mladoletnega otroka bi bila mogoča na podlagi soglasja staršev ali zakonitih zastopnikov.

Ob dopolnitvi polnoletnosti bi moral imeti posameznik pravico:

- potrditi nadaljnjo vključitev ali
- zahtevati izbris podatkov.

6.3 Prostovoljna možnost ob rojstvu

Staršem bi se ob rojstvu otroka lahko ponudila možnost vključitve v sistem.

Odločitev bi morala biti:

- popolnoma prostovoljna,
- brez kakršnih koli negativnih posledic v primeru odklonitve,
- izvedena v skladu z medicinskimi standardi.

7. QEI - BIOMETRIČNI IDENTIFIKACIJSKI TOKEN

7.1 Opredelitev

QEI (*Quantized Encrypted Identity*) predstavlja anonimiziran in kriptografsko zaščiten identifikacijski sistem, ki iz standardiziranih biometričnih predlog ustvari nepovraten identifikacijski token.

QEI ni osebni podatek v obliki imena, EMŠO ali drugega neposrednega identifikatorja, temveč tehnični kriptografski povezovalni element, ki omogoča preverjanje ujemanja ob izpolnjenih pravnih pogojih.

7.2 Ključne značilnosti

Jedro sistema bi bilo:

- biometrične predloge, ne surovi podatki,
- enotni QEI token,
- ločene evidence,
- večstopenjski dostop,
- revizijska sled,
- zasebnost po načelu *privacy by design*.

7.3 Česa QEI ne sme vsebovati

QEI token ne sme vsebovati:

- surovih slik prstnih odtisov,
- fotografij obraza,
- celotnega genetskega zapisa,
- zdravstvenih genetskih podatkov,
- prostega besedila o osebi,
- političnih, verskih ali drugih občutljivih atributov,
- neposrednih osebnih identifikatorjev.

7.4 Pravna definicija sistema QEI

QEI predstavlja anonimen, kriptografsko generiran identifikacijski token, ustvarjen iz standardiziranih biometričnih predlog, ki:

- ne vsebuje osebnih podatkov,
- ne omogoča rekonstrukcije identitete,
- ne omogoča rekonstrukcije biometrije,
- ne vsebuje zdravstvenih, dednih ali drugih občutljivih informacij.

Sistem zagotavlja:

- popolno ločitev identitetnih podatkov, biometričnih predlog in revizijskih zapisov,
- uporabo enosmernih kriptografskih funkcij,
- nepovezljivost med sistemi,
- večnivojski pravni in tehnični nadzor dostopa.

7.5 QEI - Physical Emergency Trigger Suite (PET-S)

Za primere, v katerih biometrična aktivacija ni mogoča, ni primerna ali ni pravočasno izvedljiva, se predlaga tudi dopolnilni sistem fizičnih sprožilcev brez biometrije:

QEI - Physical Emergency Trigger Suite (PET-S)

(Trije fizični načini sprožitve brez uporabe biometrije.)

7.5.1 Skupna logika (enoten sistem)

Vsi trije sprožilci delujejo po enaki logiki:

- fizična aktivacija,
- kriptografska verifikacija,
- generiranje zahtevka *Emergency Request (ER)*,
- aktivacija protokola ERAP,
- brez uporabe biometrije.

7.5.2 PET-1: QEI fizični ključek



Oblika:

- USB-C oziroma NFC ključ,
- povezan z *Family Tokenom*.

Aktivacija:

- vstavi ali prisloni se ključek,
- vnese se PIN,
- sistem sproži *Emergency Request (ER)*.

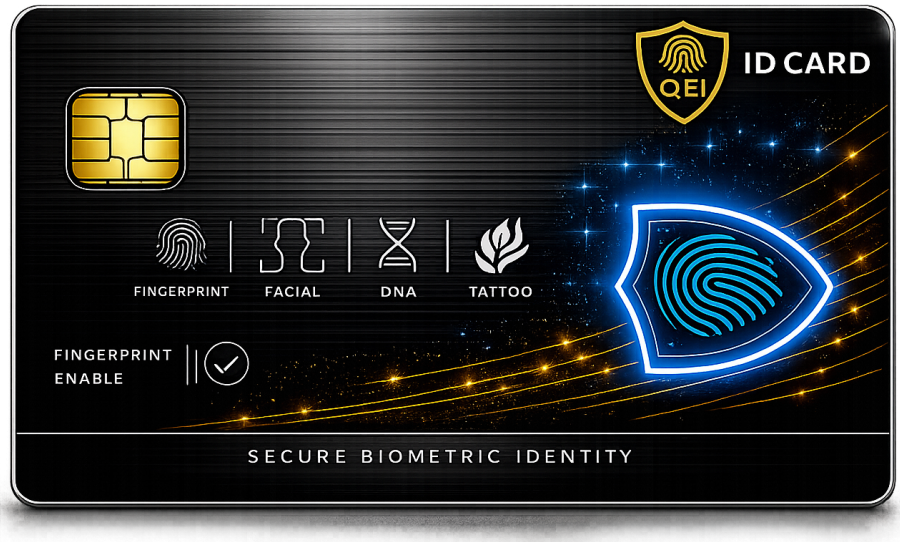
Varnost:

- varnostni čip (*Secure Element*),
- zaščita proti kloniranju (*anti-clone*),
- vezanost na družino.

Uporaba:

- starši,
- policija, če ima za to ustrezno pravno podlago in dovoljen dostop.

7.5.3 PET-2: Emergency kartica (Child ID)





Oblika:

Kartica vsebuje:

- vizualni označevalec prstnega odtisa,
- NFC čip,
- identifikator QEI (*QEI ID*).

Aktivacija:

- nekdo najde otroka,
- skenira kartico,
- sistem preveri identifikator,
- sproži signal pristojnemu organu.

Varnost:

- samo psevdonimni identifikator,
- brez osebnih podatkov.

Uporaba:

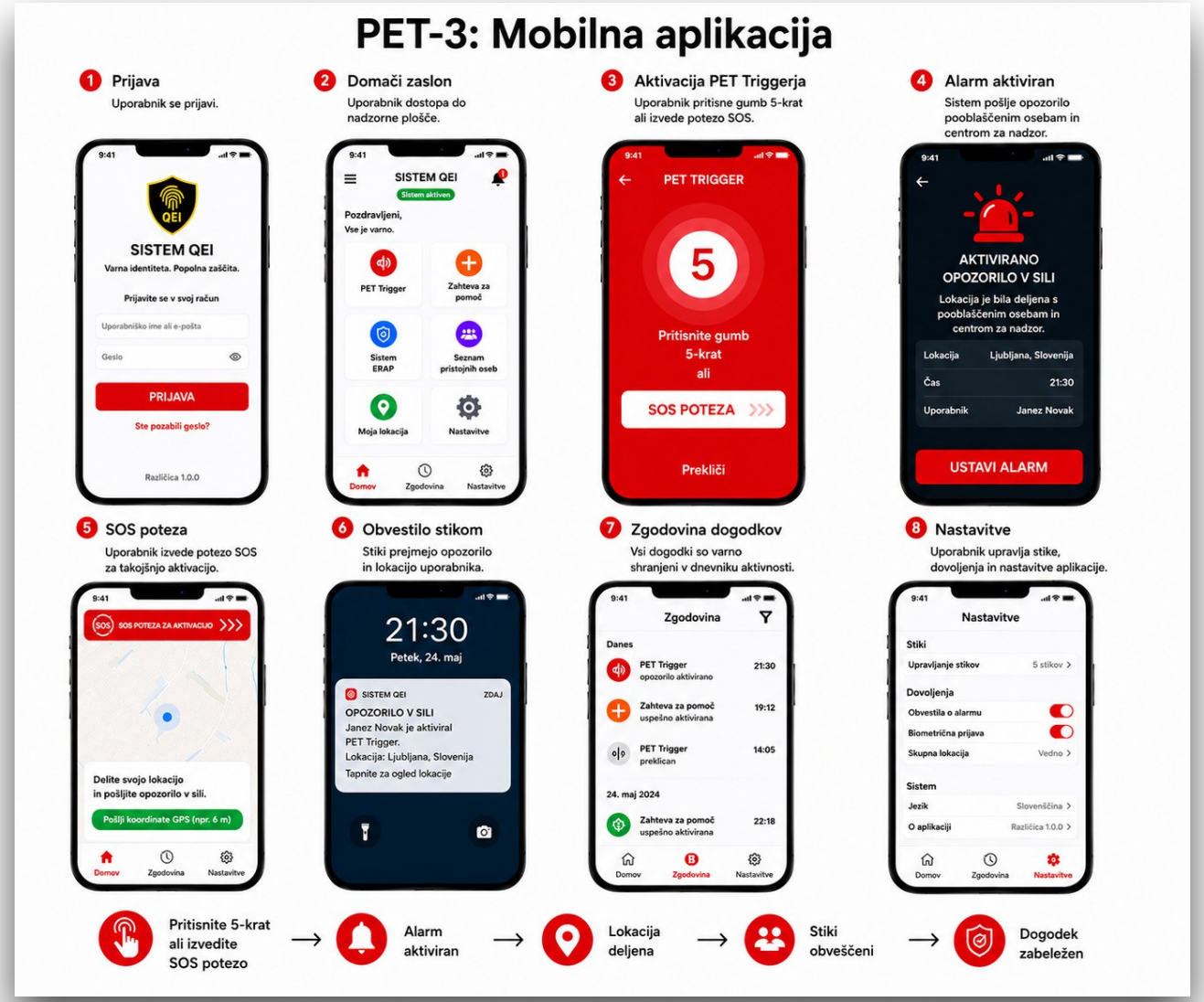
- javnost,
- pristojne institucije.

7.5.4 PET-3: Panic Trigger (naprava)

Oblika:

- funkcija v mobilnem telefonu ali QEI napravi.





Aktivacija:

- skrita kombinacija (npr. petkratni pritisk gumba),
- ali **SOS poteg (*SOS swipe*)**.

Varnost:

- omejen dostop,
- beleženje vseh aktivnosti (*logging*),
- možnost preklica.

Uporaba:

- otrok,
- starš.

7.5.5 Integracija v sistem

[PET sprožilec]

↓

[Nujna zahteva za pomoč (ER)]

↓

[Sistem ERAP]

↓

[Pristojni organi + storitve spremljanja nadzornih seznamov]

8. PREDLOG ARHITEKTURE IN PODATKOVNEGA MODELA QEI SISTEMA

8.1 Osnovna arhitektura

Predlagani sistem bi temeljil na treh ločenih plasteh.

1. Bio Layer

- biometrične predloge,
- predloga prstnega odtisa,
- obrazna predloga,
- transformiran STR-biometrični vzorec.

2. Crypto Layer

- normalizacija,
- kriptografska transformacija,
- generiranje QEI tokena,
- derivacija ključev,
- podpisni mehanizem.

3. Access Layer

- dovoljenja,
- pravna podlaga,
- revizija dostopa,
- vpogled glede na uporabniške vloge,
- obveščanje uporabnika.

8.2 Ločene evidence

Sistem bi moral temeljiti na strogi ločenosti najmanj treh evidenc.

a) Evidenca identitete

Ločena zunanja evidenca, ki lahko vsebuje:

- interno identifikacijsko številko,
- ime in priimek,
- datum rojstva,
- državljanstvo,
- status osebe,
- kontaktne ali skrbniške podatke.

QEI sistem teh podatkov ne bi smel hraniti znotraj kriptografskega tokena.

b) Biometrična evidenca

Ločena evidenca biometričnih predlog, ne surovih podatkov:

- *fingerprint template*,
- *facial template*,
- omejena transformirana STR-predloga,
- datum zajema,
- kakovost vzorca,
- vir vzorca,
- status veljavnosti.

c) QEI vezna evidenca

Ta evidenca bi vsebovala:

- QEI token,
- tehnične reference med evidencami,
- revizijske zapise.

8.3 Načelo delovanja sistema

Delovanje sistema bi potekalo po naslednjem zaporedju:

- biometrični vhod → pretvorba v predlogo
- predloga → generiranje QEI tokena ali kriptografskega materiala
- token ali ključni material → primerjava oziroma podpisni postopek
- ob ujemanju → sprožitev pravno odobrenega postopka
- šele nato → možen dostop do zunanje identitetne evidence

8.4 Pravno definirana arhitektura sistema

Sistem temelji na treh funkcionalno in pravno ločenih plasteh.

a) Bio Layer

Ta plast vsebuje izključno standardizirane biometrične predloge in nikoli ne vsebuje surovih biometričnih ali bioloških podatkov.

b) Crypto Layer

Ta plast izvaja kriptografsko transformacijo, tokenizacijo, derivacijo ključev in podpisne postopke, pri čemer uporablja enosmerne in varne kriptografske mehanizme.

c) Access Layer

Ta plast vsebuje pravila dostopa, revizijske mehanizme, pravno podlago za vpogled, sodni nadzor ter mehanizme odločanja o tem, ali je razkritje identitete sploh dopustno.

Takšna arhitektura zagotavlja funkcionalno, tehnično in pravno ločenost bistvenih elementov sistema.

9. TRILOCK - TRIFAKTORSKI VARNOSTNI MODEL

9.1 Osnovna zasnova

Najbolj smiselna, varna in sodobno zasnovana različica sistema temelji na kombinaciji treh neodvisnih biometričnih faktorjev, ki skupaj tvorijo model **TriLock**:

- **K_STR** - kriptografski material, izpeljan iz transformiranega STR-biometričnega vzorca,
- **K_FP** - kriptografski material, izpeljan iz prstnega odtisa,
- **K_FACE** - kriptografski material, izpeljan iz obrazne biometrije.

Noben od teh elementov naprave ne zapusti v surovi ali rekonstruabilni obliki.

9.2 Pragovni model uporabe

Sistem lahko uporablja večnivojski pragovni model:

- **LOW** → K_FP ali K_FACE
- **MEDIUM** → K_FP + K_FACE
- **HIGH** → K_FP + K_FACE + K_STR

Takšen model omogoča prilagoditev stopnje zaupanja glede na občutljivost posameznega postopka.

9.3 Združevanje ključev

Končni ključ se oblikuje iz več faktorjev skupaj z dodatnim kontekstom sistema:

K_FINAL = HKDF(K_STR || K_FP || K_FACE || SALT || CTX)

Pri tem velja:

- uporablja se HKDF ali drug primerljiv varen mehanizem za derivacijo ključev,
- vsak sistem uporablja svoj **SALT**,
- vsak namen uporabe uporablja svoj **CTX**,
- s tem se zagotavlja nepovezljivost med sistemi.

9.4 Ključna prednost modela

Model TriLock omogoča:

- večplastno varnost,
- bistveno manjše tveganje lažnih zadetkov,
- boljšo pravno obrambo sistema,
- večjo odpornost na zlorabe,
- višjo skladnost z načelom minimalizacije podatkov.

9.5 Način delovanja ključnega mehanizma QEI

Na konceptualni ravni sistem deluje tako, da uporabnik aktivira lokalni biometrični faktor, na primer prstni odtis, iz katerega se ustvari standardizirana biometrična predloga.

Ta se ne shrani in ne pošlje v surovi obliki, temveč se uporabi izključno kot lokalni vhod za generiranje enkratnega kriptografskega podpisa.

Postopek poteka tako, da sistem pošlje **izziv (*challenge*)**, naprava pa na podlagi lokalno preverjenih biometričnih faktorjev in konteksta ustvari enkraten kriptografski odgovor.

Rezultat je lahko:

- dostop odobren,
- dostop zavrnjen,
- zahteva za dodatni faktor.

Ključna ideja sistema je, da biometrija ne odklepa sistema kot statični identifikator, temveč sodeluje pri ustvarjanju enkratnega digitalnega ključa oziroma kriptografskega podpisa.

9.6 QEI ONE - enotni varnostni ključ

Namesto treh ločenih naprav se lahko predvidi tudi enotna fizična naprava:

QEI ONE - enotni varnostni ključ

Koncept

QEI ONE združuje:

- varnostni ključ **(*Token Access*)**,
- identifikacijo **(ID / QR / NFC)**,
- ***Panic / Emergency Trigger***.

Gre za eno fizično napravo, ki združuje več funkcij v enotnem varnostnem nosilcu.

Kako izgleda:



Naprava QEI ONE je lahko zasnovana v naslednji obliki:

- oblika kapljice (*teardrop-shaped form factor*),
- približno **9 cm** dolžine,
- približno **6 cm** širine,
- tanka in ergonomska zasnova (*slim-profile design*).

Funkcionalni sloji

Secure Core

- Secure Element (varnostni čip),
- hrani fragmente sistema QEI in kriptografski material.

NFC + QEI ID

- funkcionalnost identifikacije,
- možnost sprožitve izrednega postopka s skeniranjem **(*Emergency Scan*)**.

SOS gumb

- velik fizični gumb za sprožitev izrednega postopka,
- takoj sproži protokol **ERAP**.

LED indikator

- **zelena** = sistem deluje pravilno,
- **rdeča** = aktiviran izredni način (*Emergency Mode*),
- **modra** = naprava je aktivna oziroma povezana.

Baterija

- kompaktna vgrajena baterija,
- dolga avtonomija delovanja.

Kako deluje

Normalna uporaba

- naprava se približa čitalniku,
- NFC omogoči dostop.

Nujni primer

- pritisne se gumb SOS,
- ali se uporabi prstni odtis,
- sistem sproži protokol ERAP.

Arhitektura v eni napravi

- [QEI ONE DEVICE]
- Secure Core
- NFC ID
- SOS Trigger
- ERAP System

Prednosti

- ena naprava,
- enostavnejša uporaba,
- vedno pri uporabniku,
- večja varnost,
- več načinov sprožitve,
- ni odvisna izključno od biometrije,
- patentno močnejši koncept *multi-function hardware identity token*.

10. STR-BIOMETRIČNI VZOREC KOT DODATNI FAKTOR

10.1 Pravilna vloga STR komponente

V sistemu se DNK ne uporablja kot trajni identifikator, temveč izključno transformiran STR-biometrični vzorec, iz katerega se generira kriptografski material.

To pomeni, da sistem ne temelji na hrambi DNK, temveč na kratkotrajni tehnični transformaciji omejenega nabora identifikacijskih markerjev.

10.2 Proces obdelave

Proces lahko poteka po naslednjem modelu:

STR → numerični vektor → dodajanje SALT → transformacija → fuzzy extractor → K_STR

ali podrobneje:

STR → normalizacija → binarna reprezentacija → dodajanje SALT + CTX → randomizirana transformacija → fuzzy extractor → generiranje kriptografskega materiala K_STR

10.3 Temeljna pravila

- surovi DNK podatki se izbrišejo takoj po obdelavi,
- ne shranjuje se celoten genetski zapis,
- **K_STR** ne predstavlja identitete posameznika,
- **K_STR** se uporablja izključno kot lokalni kriptografski material,
- STR komponenta se uporablja le kot dodatni faktor za visoko stopnjo zaupanja.

10.4 Pravna prednost takšne zasnove

S tem se sistem odmika od modela **»DNK kot podatek«** in se približuje modelu **»transformiran biometrični faktor za lokalno kriptografsko uporabo«**, kar je bistveno bolj obrambno z vidika:

- varstva zasebnosti,
- načela minimalizacije,
- načela ***privacy by design***,
- omejitve namena uporabe.

11. KRIPTOGRAFSKA AVTENTIKACIJA

11.1 Načelo *challenge-response*

Sistem bi moral uporabljati kriptografski mehanizem **izziv–odgovor (*challenge-response*)**.

Postopek poteka na naslednji način:

1. Strežnik pošlje kriptografsko varen **izziv (*challenge*)**.
2. Naprava lokalno generira oziroma odklene ključ **K_FINAL**.
3. Naprava z uporabo ključa **K_FINAL** podpiše izziv.
4. Strežnik preveri podpis z ustreznim javnim ključem.

11.2 Česa sistem nikoli ne pošilja

Sistem nikoli ne pošilja:

- surove biometrije,
- biometričnih predlog,
- STR vzorca,
- tokena kot identitete.

Biometrija in tokeni se ne uporabljajo kot neposredno sredstvo avtentikacije, temveč kot lokalni sprožilni mehanizem za ustvarjanje kriptografskega podpisa.

11.3 Načelo *fail-safe*

V primeru dvoma, napake, nepopolnega ujemanja ali tehnične negotovosti sistem ne razkrije identitete posameznika.

Privzeto ravnanje sistema mora biti usmerjeno v zavrnitev dostopa oziroma zahtevo po dodatni verifikaciji in ne v razkritje identitetnih podatkov.

12. LOKALNA OBDELAVA IN VARNI MODULI

12.1 Lokalna obdelava

Sistem mora zagotavljati, da se vsi biometrični podatki obdelujejo izključno lokalno v varnem strojno-programskem okolju, kot je:

- **Trusted Execution Environment (TEE)**,
- **Secure Enclave**,
- drug primerljiv varni modul.

12.2 Prepoved iznosa biometrije

Biometrični vhodni podatki:

- ne smejo zapustiti naprave v surovi obliki,
- ne smejo zapustiti naprave v rekonstruabilni obliki,
- se ne smejo uporabljati kot globalni identifikator,
- se ne smejo prenašati v centralne baze.

12.3 Lokalna hramba ključev

Naprava mora generirati in hraniti zasebni kriptografski ključ znotraj varnega modula.

Strežniški sistemi ne smejo hraniti biometričnih podatkov ali njihovih neposrednih reprezentacij.

12.4 Brez centralne baze biometrije

Sistem ne vzpostavlja centralizirane baze biometričnih ali genetskih podatkov.

Shranjuje se izključno anonimiziran kriptografski token oziroma minimalni tehnični rezultat, ki sam po sebi ne omogoča identifikacije posameznika ali rekonstrukcije biometrije.

13. OBVEŠČANJE UPORABNIKA IN NADZOR UPORABE

13.1 Načelo transparentnosti uporabe

Vsaka uporaba sistema mora biti revizijsko zabeležena.

Zapis uporabe mora vključevati najmanj:

- čas,
- storitev oziroma postopek,
- lokacijo oziroma sistemski izvor,
- rezultat uporabe.

13.2 Obvestilo uporabniku

Kadar je to pravno in operativno dopustno, mora uporabnik prejeti obvestilo o uporabi njegovega identifikacijskega mehanizma.

Če uporaba ni bila avtorizirana s strani upravičene osebe, mora sistem omogočati:

- blokado nadaljnje uporabe,
- ponastavitev sistema oziroma zamenjavo ključnega materiala,
- preklic obstoječega ključa,
- začetek revizijskega oziroma varnostnega postopka.

13.3 Revizija in odgovornost

Sistem mora zagotavljati popolno sledljivost vseh dostopov in vseh aktivacij postopkov.

Revizijska evidenca mora vsebovati najmanj:

- kdo je dostopal,
- kdaj je dostopal,
- na podlagi katere pravne podlage,
- za kateri namen,
- kakšen je bil rezultat postopka.

Nad sistemom mora obstajati neodvisen nadzorni mehanizem, ki omogoča redno presojo zakonitosti, sorazmernosti in varnosti uporabe.

14. REVOCATION IN UPRAVLJANJE ŽIVLJENJSKEGA CIKLA IDENTITETE

14.1 Revocation

V primeru kompromitacije mora sistem omogočati zamenjavo identitetnega materiala brez spremembe bioloških lastnosti posameznika.

Postopek:

- generira se nov **SALT**,
- izvede se nova transformacija biometričnega materiala,
- ustvari se nov kriptografski ključ,
- prejšnji ključ se deaktivira.

14.2 Prednost

To pomeni, da sistem ni statičen in omogoča obnovo varnosti tudi po incidentu, kar je ena ključnih prednosti pred klasičnimi centraliziranimi biometričnimi bazami.

14.3 Upravljanje identitete brez spremembe bioloških lastnosti

Sistem omogoča ponovno generiranje identitetnega oziroma kriptografskega materiala brez potrebe po spremembi bioloških lastnosti posameznika.

To se doseže z:

- generiranjem novega **SALT**,
- uporabo novega konteksta **(CTX)**, kadar je to potrebno,
- novo kriptografsko transformacijo,
- generiranjem novega ključa,
- deaktivacijo starega ključa.

Tak mehanizem bistveno zmanjšuje tveganje trajne kompromitacije.

15. NORMATIVNE ZAHTEVE

Sistem bi moral izpolnjevati najmanj naslednje zahteve:

- biometrija se obdeluje izključno lokalno,
- STR se uporablja samo kot transformiran in neponovljiv biometrični vzorec,
- tokeni niso identiteta in se ne uporabljajo za neposredno avtentikacijo,
- avtentikacija temelji na kriptografskem podpisu,
- **SALT** mora biti unikaten za vsakega uporabnika in vsak sistem,
- **CTX** mora biti vezan na namen uporabe,
- sistem mora omogočati **revocation**,
- centralizirana baza biometričnih podatkov ni dovoljena,
- sistemi med seboj ne smejo biti kriptografsko povezljivi,
- vsak poseg mora biti sledljiv in pravno omejen.

15.1 Dodatne normativne zahteve

Sistem mora dodatno zagotavljati:

- nepovezljivost tokenov med sistemi,
- uporabo **SALT** na ravni uporabnika,
- uporabo **CTX** na ravni namena,
- večfaktorsko logiko uporabe,
- prepoved uporabe tokena kot neposredne identitete,
- pravilo minimalnega odziva sistema,
- načelo **fail-safe** ob nejasnem rezultatu,
- obvezno revizijsko sled vseh vpogledov.

16. VARNOSTNE IN PRAVNE VAROVALKE

Sistem bi moral vključevati:

- ločeno in šifrirano hrambo podatkov,
- večnivojsko šifriranje,
- dostop izključno na podlagi pravno dopustnega postopka,
- neodvisni nadzorni organ,
- letno javno poročanje,
- redne varnostne penetracijske teste,
- certificiranje po standardih informacijske varnosti,
- decentralizirane varnostne mehanizme,
- dolgoročno odpornost kriptografskih rešitev.

Vsaka zloraba ali razširitev namena uporabe bi morala biti kazniva.

17. FINANČNI IN RAZVOJNI OKVIR

17.1 Možni viri financiranja

- državni proračun,
- evropski programi,
- raziskovalni in razvojni projekti,
- javno-zasebna partnerstva, če so pravno in etično dopustna.

17.2 Okvirna ocena stroškov

Za potrebe začetne presoje izvedljivosti se lahko določi okvirna finančna ocena:

- razvoj sistema: **2–5 milijonov EUR**,
- pilotni projekt: približno **500.000 EUR**,
- letno vzdrževanje: odvisno od obsega implementacije.

Možni viri financiranja vključujejo:

- evropske programe (npr. **Horizon Europe**, **Digital Europe**, **LIFE**),
- nacionalna sredstva,
- kombinirane modele financiranja.

Pri tem je mogoče pričakovati visoko stopnjo sofinanciranja Evropske unije (do **90 %**), zlasti v okviru projektov digitalne identitete in zaščite ranljivih skupin.

17.3 Intelektualna lastnina in patentna zaščita

Predlagani sistem Q**EI (*Quantized Encrypted Identity*)** vključuje več izvirnih tehničnih, varnostnih in organizacijskih rešitev s področja biometrične identitete, kriptografije, zaščite zasebnosti, tokenizacije identitete ter varne digitalne avtentikacije.

Predlagatelj pobude je za posamezne tehnične elemente sistema pripravil oziroma vložil postopke zaščite intelektualne lastnine in patentne zaščite pri pristojnih organih za industrijsko lastnino.

Predmet zaščite lahko med drugim vključuje:

- anonimizirani biometrični identitetni sistem **QEI_TOKEN**,
- metode za generiranje kriptografskega materiala iz več neodvisnih biometričnih faktorjev,
- večfaktorski varnostni model **TriLock** (**STR + prstni odtis + obrazna biometrija**),
- sistem ločenih evidenc identitetnih podatkov, biometričnih predlog in revizijskih zapisov,
- **QEI ONE** - večnamenski fizični identifikacijski in varnostni ključ,
- **PET-S (*Physical Emergency Trigger Suite*)** za sprožanje izrednih postopkov brez uporabe biometrije,
- metode za lokalno obdelavo biometričnih podatkov brez centralizirane hrambe biometričnih podatkov,
- metode za nepovratno tokenizacijo identitete in kriptografsko verifikacijo.

Patentna zaščita ne omejuje javne, strokovne ali zakonodajne razprave o pobudi. Njen namen je zaščita inovativnih rešitev, preprečevanje nepooblaščenega prevzema intelektualne lastnine ter omogočanje nadaljnjega razvoja sistema v sodelovanju z državnimi organi, raziskovalnimi institucijami, univerzami, gospodarstvom in institucijami Evropske unije.

Predlagatelj izraža pripravljenost za sodelovanje z **Republiko Slovenijo**, institucijami **Evropske unije** ter mednarodnimi organizacijami pri nadaljnji strokovni, pravni in tehnični presoji sistema.

V primeru nadaljnjega razvoja in morebitne implementacije sistema se lahko uporabi ustrezen model licenciranja, javno-zasebnega partnerstva, raziskovalnega sodelovanja ali drug pravno dopusten model prenosa tehnologije, ki zagotavlja zaščito javnega interesa, človekovih pravic in zaščite otrok.

Vsi nadaljnji razvojni postopki morajo potekati v skladu z veljavno zakonodajo Republike Slovenije, pravom Evropske unije, mednarodnimi standardi informacijske varnosti ter načeli varstva osebnih podatkov in zasebnosti.

18. JAVNA PREDSTAVITEV IN OBVEŠČANJE JAVNOSTI

V primeru nadaljnje obravnave pobude bi bilo treba zagotoviti transparentno javno predstavitev sistema.

Javna predstavitev bi morala vključevati sodelovanje:

- ustavnih pravnikov,
- strokovnjakov za varstvo osebnih podatkov,
- bioetikov,
- predstavnikov civilne družbe,
- strokovnjakov za zaščito otrok,
- informatikov in kriptografskih strokovnjakov.

Poseben poudarek bi moral biti namenjen pojasnilu:

- stroge namenske omejitve,
- tehničnih in varnostnih zaščit,

- prostovoljnosti vključitve,
- možnosti izbrisa,
- sodnega in neodvisnega nadzora.

Sistem ne sme biti predstavljen kot splošni nadzorni mehanizem, temveč izključno kot poseben zaščitni instrument za zaščito otrok.

19. PREDLOG NADALJNJIH KORAKOV

Predlagamo:

- organizacijo javne razprave na nacionalni ravni,
- pripravo strokovne analize ustavne skladnosti,
- pripravo presoje skladnosti z GDPR in pravom Evropske unije,
- pripravo tehnične študije izvedljivosti,
- vključitev domačih in mednarodnih strokovnjakov,
- preučitev možnosti pilotnega modela, če bi bil pravno dopusten,
- nadaljnjo razpravo o morebitni evropski razsežnosti pobude.

Ob morebitni uspešni implementaciji v Republiki Sloveniji bi se lahko pobuda v prihodnje predstavila tudi na ravni Evropske unije ter kasneje kot širša mednarodna pobuda za zaščito otrok.

19.1 Strateška usmeritev nadaljnjih korakov

Za uspešno nadaljnjo obravnavo pobude je smiselno poudariti, da cilj ni neposredna uvedba sistema brez predhodne presoje, temveč:

- strokovna analiza,
- pravna validacija,
- tehnična študija izvedljivosti,
- pilotni model, če je pravno dopusten.

Najmočnejši pristop ni **»uvedimo sistem«**, temveč **»preučimo sistem kot dopolnilni zaščitni mehanizem za izjemne primere«**.

Takšna usmeritev:

- zmanjšuje odpor,
- povečuje pravno sprejemljivost,
- omogoča institucionalno podporo,
- odpira možnost financiranja na ravni Evropske unije.

Osrednji namen pobude je krepitev zaščite otrok. Tehnološke rešitve predstavljajo zgolj podporno sredstvo za doseganje tega cilja in morajo biti vedno podrejene varstvu človekovih pravic, zasebnosti ter največji koristi otroka.

Ključno sporočilo pobude je naslednje:

Če obstaja tehnologija, ki lahko reši življenje pogrešanega otroka, je dolžnost države, da vsaj preveri njeno ustavno, pravno in tehnično izvedljivost.

19.2 Predlog pilotnega projekta

Za prehod iz konceptualne ravni v operativno preverjanje se predlaga izvedba pilotnega projekta.

Možni okvir pilotnega projekta:

- **obseg**: 100-500 otrok,
- **trajanje**: 12 mesecev.

Vključitev:

- ena bolnišnica,
- ena policijska enota,
- omejeno število prostovoljnih družin.

Cilji pilotnega projekta:

- preveriti tehnično izvedljivost,
- preveriti pravno skladnost v praksi,
- oceniti uporabniško izkušnjo,
- preveriti varnostne mehanizme,
- identificirati morebitna tveganja.

Pilotni projekt bi predstavljal ključen korak pred morebitno širšo implementacijo.

20. URADNI PREDLOG ZA VLADO REPUBLIKE SLOVENIJE

Predlagamo, da **Vlada Republike Slovenije** preuči možnost začetka strokovne in javne razprave o vzpostavitvi posebnega, strogo omejenega in prostovoljnega identifikacijskega sistema, katerega izključni namen bi bil zaščita otrok pred:

- trgovino z otroki,
- krajo otrok ob rojstvu,
- suženjstvom,
- spolnim izkoriščanjem,
- nezakonitimi posvojitvami,
- drugimi posebej hudimi posegi v pravice otrok.

Vsaka morebitna rešitev mora biti:

- strogo namensko omejena,
- pod sodnim in neodvisnim nadzorom,
- v skladu z **Ustavo Republike Slovenije**,
- v skladu z **evropsko zakonodajo**,
- tehnično zasnovana tako, da preprečuje zlorabe.

21. PRAVNI ARGUMENTI ZA NADALJNJO STROKOVNO RAZPRAVO

21.1 Razširjeni pravni argumenti

Argumenti ZA

- varstvo otrok kot ustavno zaščitena vrednota,
- hitrejša identifikacija pogrešanih otrok,
- krepitev pravne varnosti v posebej občutljivih postopkih,
- preprečevanje organiziranega kriminala,
- večja možnost preverjanja identitete v izrednih primerih.

Argumenti PROTI

- poseg v pravico do zasebnosti,
- posebna občutljivost biometričnih in genetskih podatkov,
- vprašanje sorazmernosti,
- tveganje varnostnih vdorov ali zlorab,
- nevarnost poznejše širitve namena uporabe.

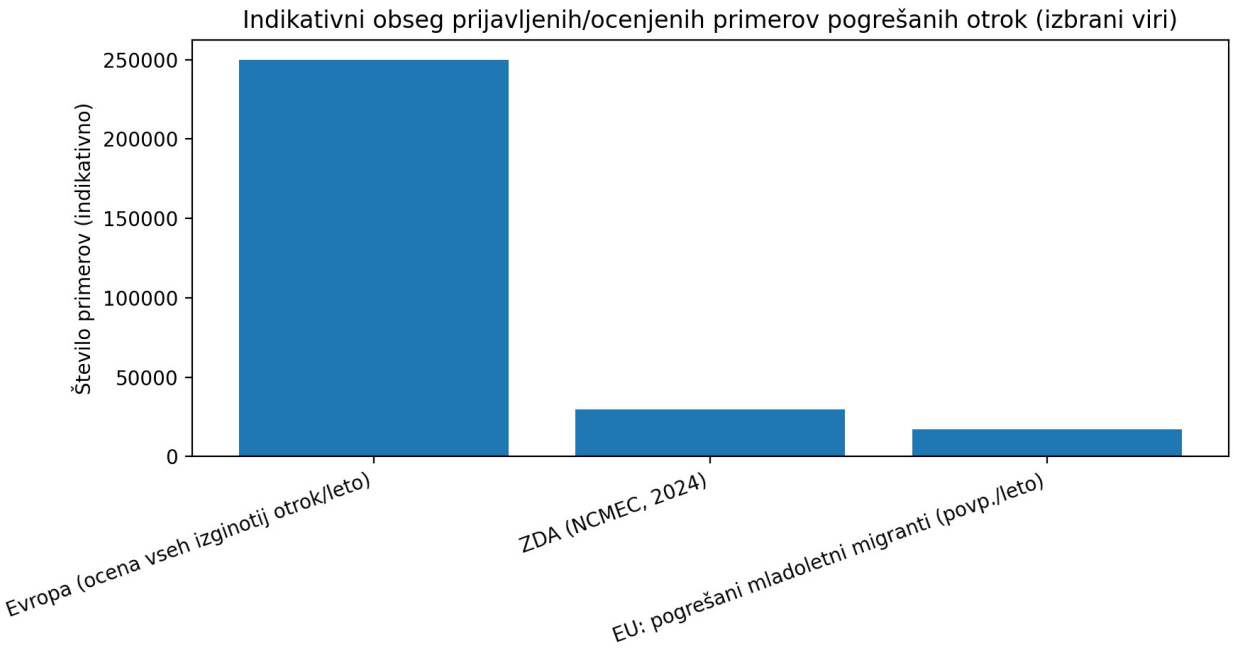
Prav zato mora biti vsaka nadaljnja razprava strogo pravno utemeljena, tehnično preverljiva in popolnoma transparentna.

22. INDIKATIVNI STATISTIČNI PREGLED IN DODATKI

To poglavje predstavlja pregled javno dostopnih mednarodnih podatkov, ki ponazarjajo razsežnost problematike pogrešanih otrok, ugrabitev otrok ter trgovine z ljudmi. Zaradi različnih pravnih opredelitev, metodologij zbiranja podatkov in nacionalnih evidenc neposredna primerjava med posameznimi državami ni vedno mogoča. Namen prikazanih podatkov je predstaviti okvirno razsežnost problematike in podpreti strokovno razpravo o potrebi po dodatnih zaščitnih mehanizmih za otroke.

22.1 Indikativni statistični pregled

Za boljše razumevanje razsežnosti obravnavane problematike so v nadaljevanju predstavljeni izbrani statistični kazalniki iz **Združenih držav Amerike**, **Evrope** in **svetovnega okolja**. Pregled temelji na podatkih **Nacionalnega centra za pogrešane in izkoriščane otroke (National Center for Missing & Exploited Children - NCMEC)**, **Nacionalnega informacijskega centra za kriminal (National Crime Information Center - NCIC)**, **organizacije Missing Children Europe**, **Evropske unije** ter **Urada Združenih narodov za droge in kriminal (United Nations Office on Drugs and Crime - UNODC).**



Prikazani podatki kažejo, da problematika pogrešanih otrok, ugrabitev in trgovine z ljudmi predstavlja globalni izziv. Čeprav se metodologije zbiranja podatkov med državami razlikujejo, vsi razpoložljivi viri potrjujejo potrebo po nadaljnjem razvoju učinkovitih zaščitnih mehanizmov za otroke.

Regija	**Pogrešani / izginuli otroci**	**Ugrabitve / abdukcije**	**Trgovina z ljudmi / otroki**
ZDA	• NCMEC (2024): **29.568** prijav pogrešanih otrok. • NCIC (2024): **349.557** prijav pogrešanih oseb.	• **2.366** ugrabitev s strani starša brez skrbništva. • **293** ugrabitev s strani neznane osebe.	• Približno **1 od 7** primerov ogroženih pobegov je povezan s tveganjem trgovine z ljudmi.
Evropa	• Približno **250.000** prijav pogrešanih otrok letno. • 2021–2023: najmanj **51.433** pogrešanih mladoletnih migrantov.	• Ni enotne statistike EU; podatki so razdrobljeni med državami.	• UNODC poroča o različnih oblikah izkoriščanja otrok; deleži se razlikujejo med državami.
Globalno	• Ni enotne primerljive svetovne statistike.	• Ni enotne globalne statistike ugrabitev otrok.	• UNODC (2022): **69.627** zaznanih žrtev trgovine z ljudmi; otroci predstavljajo približno **38 %** zaznanih žrtev.

Opomba: Podatki so indikativni in namenjeni primerjalnemu prikazu. Zaradi razlik v pravnih opredelitvah in metodologijah neposredna primerjava med državami ni vedno mogoča.

Viri: NCMEC, NCIC, Missing Children Europe, Evropska unija, UNODC – *Globalno poročilo o trgovini z ljudmi*.

22.2 Ugrabitve oziroma odtujitve novorojenčkov iz porodnišnic

Ugrabitve oziroma odtujitve novorojenčkov iz porodnišnic sodijo med najbolj občutljive oblike kaznivih dejanj nad otroki. Takšni primeri so v večini razvitih držav statistično redki, vendar imajo zaradi trajnih posledic za otroka, starše in družbo izjemno velik pomen.

Zaradi neenotnih pravnih opredelitev, različnih načinov poročanja in razdrobljenih evidenc trenutno ne obstaja enotna svetovna statistika, ki bi omogočala neposredno primerjavo med državami. Posamezne države vodijo evidence po različnih merilih, zato so mednarodne primerjave omejene.

Ne glede na njihovo redkost predstavljajo takšni primeri eno najtežjih oblik posega v pravice otroka. Zato številni strokovnjaki poudarjajo pomen preventivnih ukrepov, hitre identifikacije otrok ter učinkovitega sodelovanja med zdravstvenimi ustanovami, policijo, pravosodnimi organi in centri za socialno delo.

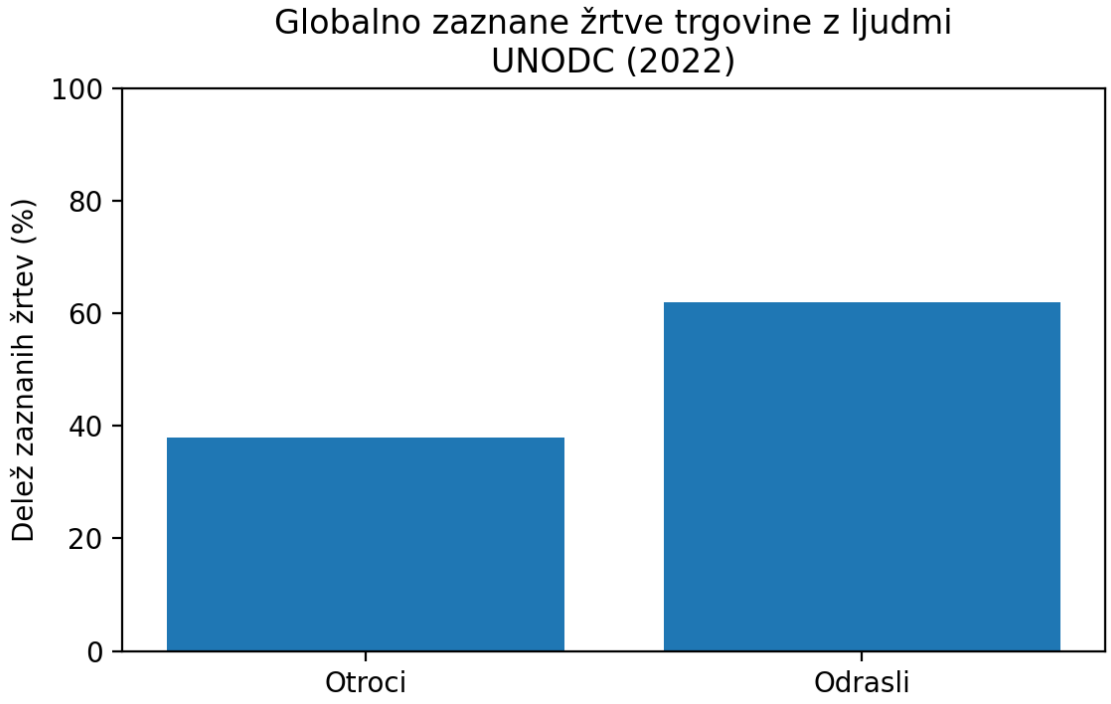
Predlagani sistem QEI je zasnovan kot prostovoljen, strogo zakonsko omejen in zasebnostno varovan zaščitni mehanizem, katerega namen ni nadzor posameznikov, temveč hitrejša pomoč pri identifikaciji otrok v izjemnih primerih ugrabitve, nezakonite odtujitve ali trgovine z ljudmi.

Čeprav so takšni primeri statistično redki, njihove posledice za otroka, družino in družbo upravičujejo razmislek o dodatnih zaščitnih mehanizmih, ki bi ob spoštovanju človekovih pravic, zasebnosti in načela prostovoljnosti omogočili hitrejšo identifikacijo otroka v izjemnih okoliščinah.

22.3 Globalna trgovina z ljudmi - delež otrok

Trgovina z ljudmi ostaja ena najhujših oblik organiziranega kriminala in ena najresnejših kršitev človekovih pravic. Otroci predstavljajo posebno ranljivo skupino, saj so pogosto žrtve spolnega izkoriščanja, prisilnega dela, prisilnega beračenja, nezakonitih posvojitev ter drugih oblik izkoriščanja.

Po podatkih **Organizacije združenih narodov (UNODC)** je bilo leta **2022** po svetu evidentiranih **69.627 zaznanih žrtev trgovine z ljudmi**, pri čemer so otroci predstavljali približno **38 % vseh zaznanih žrtev**.



Slika: Delež otrok in odraslih med zaznanimi žrtvami trgovine z ljudmi (UNODC, 2022).

Kazalnik	**Vrednost**
Evidentirane žrtve trgovine z ljudmi (UNODC, 2022)	**69.627**
Delež otrok med zaznanimi žrtvami	**38 %**
Delež odraslih med zaznanimi žrtvami	**62 %**

Vir: United Nations Office on Drugs and Crime (UNODC), Global Report on Trafficking in Persons 2024.

22.4 Viri za spremno gradivo / opombe

Podatki, navedeni v poglavju 22, temeljijo na javno dostopnih poročilih, uradnih statističnih evidencah in publikacijah mednarodnih organizacij. Zaradi različnih pravnih opredelitev, metodologij zbiranja podatkov in nacionalnih sistemov evidentiranja neposredna primerjava med posameznimi državami ni vedno mogoča. Namen navedenih virov je zagotoviti strokovno podlago za razpravo o zaščiti otrok ter ponazoriti razsežnost obravnavane problematike.

Uporabljeni viri:

1. National Center for Missing & Exploited Children (NCMEC)

- Missing Children Statistics
- Annual Reports
- CyberTipline Reports
- https://www.missingkids.org

2. National Crime Information Center (NCIC) / Federal Bureau of Investigation (FBI)

- Missing Person and Unidentified Person Statistics
- https://www.fbi.gov
- https://www.cjis.gov

3. Missing Children Europe

- Annual Data Reports
- Cross-border Missing Children Statistics
- https://missingchildreneurope.eu

4. Evropska unija

- European Parliament Research Service (EPRS)
- Disappearance of Migrant Children in the European Union
- European Commission
- Eurostat
- https://europa.eu

5. United Nations Office on Drugs and Crime (UNODC)

- Global Report on Trafficking in Persons 2024
- https://www.unodc.org

6. United Nations Children's Fund (UNICEF)

- Child Protection
- Children on the Move
- https://www.unicef.org

7. International Labour Organization (ILO)

- Global Estimates of Child Labour
- https://www.ilo.org

8. International Organization for Migration (IOM)

- Missing Migrants Project
- Human Trafficking Data
- https://www.iom.int

Metodološka opomba

Številčni podatki, uporabljeni v tem dokumentu, predstavljajo **indikativni pregled javno dostopnih informacij** in ne predstavljajo enotne mednarodne statistike. Razlike med državami izhajajo iz različnih pravnih definicij, nacionalnih evidenc, metodologij zbiranja podatkov ter načinov poročanja pristojnih organov. Posledično neposredna primerjava med posameznimi državami ni vedno metodološko primerna.

Namen prikazanih podatkov ni priprava popolne statistične analize, temveč predstavitev razsežnosti problematike pogrešanih otrok, ugrabitev otrok ter trgovine z ljudmi kot strokovne podlage za razpravo o uvedbi dodatnih zaščitnih mehanizmov.

23. SKLEP

Gre za pobudo za razmislek, strokovno presojo in javno razpravo o morebitni zakonodajni ureditvi posebej občutljivega področja zaščite otrok.

Cilj pobude ni vzpostavitev splošnega nadzornega sistema, temveč preučitev možnosti razvoja strogo omejenega, ustavno skladnega, tehnično varnega in pravno nadzorovanega zaščitnega mehanizma, ki bi bil namenjen izključno zaščiti otrok v najtežjih in najbolj občutljivih primerih.

Predlagani tehnični model temelji na združitvi treh neodvisnih biometričnih faktorjev v enoten kriptografski ključ, ki obstaja izključno na napravi uporabnika in ga ni mogoče preprosto ukrasti, kopirati ali uporabiti zunaj strogo določenega sistema.

Vsaka morebitna nadaljnja obravnava takšnega sistema mora temeljiti na:

- prostovoljnosti,
- minimalizaciji podatkov,
- nepovratni tokenizaciji,
- ločenosti evidenc,
- sodnem nadzoru,
- neodvisni reviziji,
- polnem spoštovanju človekovih pravic.

Dodatno je treba poudariti, da predlagani sistem ni namenjen povezovanju obstoječih državnih evidenc niti vzpostavitvi centralizirane zbirke biometričnih ali genskih podatkov. Sistem je zasnovan kot decentraliziran, uporabniško voden mehanizem, ki omogoča preverjanje identitete izključno v izjemnih primerih, kjer obstoječi sistemi ne zagotavljajo zanesljive identifikacije, in le na podlagi ustrezne pravne podlage.

Predlagana pobuda zato ne predstavlja predloga za takojšnjo uvedbo novega sistema, temveč poziv k odgovorni, strokovni in transparentni razpravi o možnostih razvoja dodatnega zaščitnega mehanizma, ki bi ob strogem spoštovanju človekovih pravic, varstva zasebnosti in veljavnega pravnega reda lahko prispeval k učinkovitejši zaščiti otrok.

Končna odločitev o morebitni nadaljnji pripravi zakonodaje ali izvedbi pilotnega projekta mora temeljiti na strokovnih analizah, pravni presoji, tehnični izvedljivosti ter širokem družbenem soglasju. Le na ta način je mogoče zagotoviti, da bodo morebitne prihodnje rešitve hkrati učinkovite, sorazmerne, ustavno skladne in usmerjene v največjo korist otroka.

24. VIRI IN LITERATURA

24.1 Mednarodni pravni akti

- Splošna deklaracija človekovih pravic (Organizacija združenih narodov, 1948).
- Konvencija Združenih narodov o otrokovih pravicah (1989).
- Evropska konvencija o človekovih pravicah.
- Listina Evropske unije o temeljnih pravicah.

24.2 Evropska zakonodaja

- Splošna uredba o varstvu podatkov (**GDPR**).
- Uredba o evropski digitalni identiteti (**eIDAS**).
- Akt Evropske unije o umetni inteligenci (**AI Act**).

24.3 Nacionalna zakonodaja Republike Slovenije

- Ustava Republike Slovenije.
- Zakon o varstvu osebnih podatkov (**ZVOP-2**).
- Kazenski zakonik (**KZ-1**).
- Zakon o kazenskem postopku (**ZKP**).
- Družinski zakonik.
- Zakon o nalogah in pooblastilih policije (**ZNPPol**).

24.4 Mednarodni standardi in strokovne smernice

Pri pripravi pobude so bila upoštevana tudi splošno priznana načela in priporočila s področja:

- informacijske in kibernetske varnosti,
- varstva osebnih podatkov,
- zaščite biometričnih podatkov,
- kriptografskih metod,
- digitalne identitete,
- zaščite otrok,
- preprečevanja trgovine z ljudmi.

Pri tem so bila upoštevana priporočila in standardi mednarodnih organizacij, kot so:

- Mednarodna organizacija za standardizacijo (**ISO**),
- Evropska agencija za kibernetsko varnost (**ENISA**),
- Nacionalni inštitut za standarde in tehnologijo Združenih držav Amerike (**NIST**),
- Europol,
- Interpol,
- UNICEF,
- Organizacija za gospodarsko sodelovanje in razvoj (**OECD**),
- Organizacija Združenih narodov (**UN**).

24.5 Strokovna literatura

Pri pripravi pobude so bila upoštevana tudi splošno priznana strokovna dela s področja:

- kriptografije,
- informacijske varnosti,
- digitalne identitete,
- zaščite zasebnosti,
- biometričnih sistemov,
- varstva otrok in človekovih pravic.

Opomba

Predlagana pobuda temelji na veljavni zakonodaji R**epublike Slovenije**, pravu **Evropske unije**, mednarodnih konvencijah ter splošno priznanih strokovnih načelih s področja varstva človekovih pravic, zaščite otrok, digitalne identitete, informacijske varnosti in varstva osebnih podatkov.

25. SLOVAR KLJUČNIH POJMOV, KRATIC IN TUJK

Za lažje razumevanje pobude so v nadaljevanju pojasnjeni najpomembnejši strokovni izrazi, kratice in tuji izrazi, uporabljeni v tem dokumentu.

QEI (Quantized Encrypted Identity)
Kriptografsko zaščiten identifikacijski sistem, ki iz standardiziranih biometričnih predlog ustvari anonimiziran identifikacijski token za preverjanje identitete v strogo omejenih postopkih.

Token
Kriptografski oziroma tehnični identifikacijski zapis, ki sam po sebi ne vsebuje neposredne identitete posameznika.

Biometrija
Uporaba edinstvenih telesnih ali vedenjskih značilnosti posameznika (npr. prstni odtis, obraz, šarenica ali glas) za preverjanje ali potrditev identitete.

Biometrična predloga
Standardiziran tehnični zapis določenih biometričnih značilnosti, ki ni enak surovemu biometričnemu podatku.

Biometrični identifikacijski token
Anonimiziran kriptografski identifikator, ustvarjen iz standardiziranih biometričnih predlog, ki ne vsebuje osebnih podatkov in ne omogoča rekonstrukcije biometrije ali neposredne identifikacije posameznika.

STR (Short Tandem Repeat)
Kratek ponavljajoči se odsek DNK, ki se lahko v transformirani obliki uporabi kot dodatni biometrični faktor.

Kriptografija
Veda o metodah zaščite podatkov z uporabo matematičnih algoritmov, ki zagotavljajo zaupnost, celovitost in verodostojnost informacij.

Kriptografski ključ
Digitalna vrednost, uporabljena za šifriranje, preverjanje pristnosti ali izpeljavo drugih varnostnih ključev.

Kriptografska tokenizacija
Postopek pretvorbe biometričnih ali drugih vhodnih podatkov v nepovraten kriptografski zapis, ki omogoča preverjanje ujemanja brez razkritja izvornih podatkov.

Hash funkcija (kriptografska zgoščevalna funkcija)
Matematična funkcija, ki vhodne podatke pretvori v enoličen in nepovraten zapis fiksne dolžine.

Nepovratna transformacija
Kriptografski postopek, pri katerem iz ustvarjenega rezultata ni mogoče rekonstruirati izvornih podatkov.

Avtentikacija
Postopek preverjanja, ali je oseba, naprava ali sistem res tisti, za katerega se predstavlja.

Večfaktorska avtentikacija
Način preverjanja identitete, pri katerem se za potrditev dostopa uporabita dva ali več neodvisnih varnostnih dejavnikov.

Avtorizacija
Postopek določanja, do katerih podatkov ali funkcij ima uporabnik po uspešni avtentikaciji dovoljen dostop.

Revizijska sled
Elektronski zapis vseh dostopov, preverjanj in uporabe sistema, ki omogoča naknadni nadzor zakonitosti in sledljivosti postopkov.

Ločene evidence
Načelo, po katerem so identitetni podatki, biometrične predloge in revizijski zapisi shranjeni v medsebojno ločenih evidencah, s čimer se bistveno zmanjša tveganje zlorab in nepooblaščenega dostopa.

Decentralizirana arhitektura
Arhitektura informacijskega sistema, pri kateri občutljivi podatki niso shranjeni v eni centralni zbirki, temveč so ločeni in zaščiteni v različnih varnostnih plasteh oziroma evidencah.

Decentralizirana identiteta (DID – Decentralized Identity)
Model digitalne identitete, pri katerem uporabnik ohrani nadzor nad svojo identiteto brez centralnega upravljavca.

Verifiable Credentials (VC)
Digitalna dokazila oziroma poverilnice, katerih pristnost je mogoče kriptografsko preveriti.

Root of Trust
Temelj zaupanja sistema; pravni ali tehnični okvir, ki zagotavlja verodostojnost in varnost delovanja sistema.

Challenge–Response (kriptografski izziv–odgovor)
Varnostni mehanizem, pri katerem sistem pošlje kriptografski izziv, naprava pa vrne preverljiv kriptografski odgovor.

Threat Model (model groženj)
Strukturirana analiza možnih groženj, napadov in zlorab sistema.

Deepfake
Z umetno inteligenco ustvarjena ali spremenjena digitalna vsebina, ki lahko lažno prikazuje obraz, glas ali identiteto posameznika.

Privacy by Design
Načelo, po katerem je varstvo zasebnosti vključeno že v samo zasnovo sistema.

Privacy by Default
Načelo, po katerem so privzete nastavitve sistema že od začetka usmerjene v najvišjo možno zaščito zasebnosti.

Psevdonimizacija
Postopek, pri katerem se osebni podatki nadomestijo z identifikatorjem, tako da brez dodatnih informacij posameznika ni mogoče neposredno določiti.

Anonimizacija
Postopek trajne odstranitve možnosti identifikacije posameznika, pri katerem identitete ni več mogoče ugotoviti.

Secure Enclave
Varen izoliran procesorski modul, namenjen lokalni obdelavi občutljivih podatkov in varni hrambi kriptografskih ključev.

Trusted Execution Environment (TEE)
Zaupanja vredno izvajalno okolje, ki omogoča zaščiteno izvajanje varnostno občutljivih postopkov ločeno od preostalega sistema.

Secure Element
Poseben varnostni čip, namenjen zaščiteni hrambi kriptografskih ključev in izvajanju občutljivih varnostnih postopkov.

Revocation (preklic)
Postopek preklica oziroma razveljavitve identifikacijskega ali kriptografskega elementa.

Recovery (obnova sistema)
Postopek ponovne vzpostavitve dostopa ali obnove sistema po izgubi, kraji ali kompromitaciji.

HKDF (HMAC-based Key Derivation Function)
Kriptografska metoda za varno izpeljavo novih ključev iz obstoječega kriptografskega materiala.

SALT
Naključna vrednost, dodana podatkom pred kriptografsko obdelavo, ki povečuje varnost in preprečuje predvidljive rezultate.

CTX (Context)
Kontekst uporabe, vezan na določen namen ali okolje, ki preprečuje povezovanje rezultatov med različnimi sistemi.

Pilotni projekt
Omejen preizkus sistema v praksi z namenom preverjanja njegove tehnične, pravne in operativne izvedljivosti.

ERAP (Emergency Response Activation Protocol)
Protokol za sprožitev postopkov v nujnih oziroma izrednih primerih.

Emergency Request (ER)
Kriptografsko zaščiten zahtevek za sprožitev nujnega postopka v okviru sistema QEI.

PET-S (Physical Emergency Trigger Suite)
Skupek fizičnih sprožilcev za nujne primere, ki omogočajo aktivacijo sistema brez uporabe biometrije.

Family Token
Kriptografski identifikacijski element, namenjen povezovanju članov iste družine v okviru sistema QEI brez razkritja njihove identitete.

TriLock
Večfaktorski varnostni model, ki združuje tri neodvisne biometrične dejavnike (transformirani STR-biometrični vzorec, prstni odtis in obrazno biometrijo) za ustvarjanje enotnega kriptografskega ključa.

QEI ONE
Predlagana večnamenska varnostna naprava, ki združuje identifikacijo, kriptografsko zaščito in funkcije za sprožitev postopkov v nujnih primerih.

Logging (beleženje dogodkov)
Samodejno zapisovanje vseh pomembnih varnostnih dogodkov, dostopov in postopkov za zagotavljanje sledljivosti in nadzora.

Zero Trust
Varnostni model, pri katerem nobena naprava ali uporabnik nista samodejno zaupanja vredna, temveč se vsaka zahteva posebej preveri.

Fail-safe
Način delovanja sistema, pri katerem sistem ob napaki preide v varno stanje in ne ogrozi varnosti ali zasebnosti.

Interoperabilnost
Sposobnost različnih sistemov, da med seboj tehnično in pravno usklajeno sodelujejo.

Interoperabilni standard
Dogovorjen tehnični standard, ki omogoča povezljivost in sodelovanje različnih informacijskih sistemov.

API (Application Programming Interface)
Standardiziran programski vmesnik, ki omogoča varno komunikacijo med različnimi informacijskimi sistemi.

eIDAS 2.0
Evropski pravni okvir za elektronsko identiteto, elektronsko identifikacijo in storitve zaupanja.

GDPR (General Data Protection Regulation)
Splošna uredba Evropske unije o varstvu osebnih podatkov, ki določa pravila zakonite obdelave osebnih podatkov.

Načelo najmanjših privilegijev (Least Privilege)
Načelo informacijske varnosti, po katerem ima vsak uporabnik ali sistem le tista dovoljenja, ki jih nujno potrebuje za izvajanje svojih nalog.

PRILOGA I - DODATNA STROKOVNA DOPOLNITEV: MANJKAJOČI KLJUČNI ELEMENTI ZA REALNO IZVEDBO

I.1 Root of Trust

Sedanja konceptualna raven predvideva certifikacijski oziroma potrditveni sloj, vendar mora biti za pravno in sistemsko verodostojnost jasno določeno, kdo dejansko predstavlja **temelj zaupanja** (**Root of Trust**) **sistema**.

Ključno vprašanje je:

- ali je temelj zaupanja država,
- ali gre za evropski okvir zaupanja,
- ali je možen zasebni, vendar strogo regulirani subjekt,
- ali mora biti sistem vezan na okvir **eIDAS**.

Brez jasno določenega ***Root of Trust*** ni mogoče zagotoviti:

- pravne veljavnosti podpisov,
- institucionalnega zaupanja,
- medsebojnega priznavanja rezultatov,
- operativne uporabe v uradnih postopkih.

Zato je treba v nadaljnji strokovni fazi jasno določiti, da bi moral biti temelj zaupanja umeščen znotraj:

- državnega pravnega reda,
- evropskega okvira elektronske identitete,
- ali drugega zakonsko določenega sistema visoke ravni zaupanja.

I.2 Pravna podlaga (GDPR + eIDAS + nacionalni okvir)

Ni dovolj, da sistem ne hrani surovih podatkov. Pravo namreč ne ureja le hrambe, temveč tudi:

- obdelavo,
- namen,
- pravno podlago,
- upravljavca,
- pravice posameznika,
- varnostne ukrepe,
- postopke izbrisa in preklica.

Zato bi morala vsaka nadaljnja različica projekta izrecno opredeliti:

- pravno podlago po **6. členu GDPR**,
- pravno podlago za obdelavo posebnih vrst podatkov po **9. členu GDPR**,
- razmerje do javnega interesa,
- razmerje do izrecne privolitve,
- vprašanje upravljavca in obdelovalca,

- pravico do izbrisa,
- pravico do obveščenosti,
- pravico do revizije posegov,
- razmerje do prihodnjega okvira **eIDAS 2.0**.

I.3 Upravljanje ključev (Key Management)

Ena najpomembnejših praktičnih odprtih točk sistema je upravljanje ključev in življenjskega cikla identitetnega materiala.

Odgovoriti je treba najmanj na vprašanja:

- kaj se zgodi, če uporabnik izgubi token,
- ali izgubi dostop do svoje identitete,
- kako poteka obnova,
- kako se izvede preklic,
- kako se prepreči zloraba po kraji ali kompromitaciji.

Zato mora sistem nujno predvidevati:

- mehanizem **obnove** (*recovery*),
- mehanizem **preklica** (*revocation*),
- večfaktorski postopek obnove,
- možnost vključitve družinskega ali institucionalnega potrditvenega modela,
- časovno in pravno sledljivo deaktivacijo kompromitiranega tokena.

I.4 Standardi in interoperabilnost

Trenutno je sistem opisan kot samostojen konceptualni okvir. Za realno uporabo pa mora biti sposoben interoperabilnosti z obstoječimi sistemi.

Treba je opredeliti vsaj:

- format tokena,
- standarde prenosa,
- API mehanizme,
- pravila komunikacije,
- združljivost z državnimi sistemi,
- skladnost z evropskimi digitalnimi identitetnimi okviri.

Če sistem ni interoperabilen, ostane zaprt koncept brez realne uporabnosti v:

- policijskih postopkih,
- čezmejnih primerih,
- bolnišničnem okolju,
- upravnih postopkih,
- evropskih interoperabilnih sistemih.

I.5 Verifikacijski tok (Verification Flow)

Za pravno in tehnično verodostojnost ni dovolj opis samega tokena. Natančno je treba opredeliti tudi postopek preverjanja identitete.

Opisati je treba:

- kdo začne postopek,
- kdo vidi posamezne fragmente,
- kdo jih sestavi,
- kdo preveri kriptografski rezultat,
- kdo lahko sproži dostop do identitetne evidence,
- pod katerimi pogoji se identiteta sploh razkrije.

To pomeni, da mora nadaljnji dokument vsebovati natančen postopkovni verifikacijski tok za vsak ključni scenarij uporabe.

I.6 Napadi in zlorabe

Vsak resen institucionalni ali evropski pregled bo med prvimi vprašanji odprl področje groženj, napadov in možnih zlorab.

Treba je opredeliti najmanj:

- krajo tokena,
- kloniranje naprave,
- napade s poskušanjem gesel oziroma ključev,
- napade na komunikacijo,
- socialni inženiring,
- kompromitacijo potrditvenega organa,
- napade na uporabniško napravo,
- notranje zlorabe sistema.

Zato mora biti nadaljnji razvoj dopolnjen z:

- formalnim **modelom groženj (*Threat Model*)**,
- varnostno arhitekturo,
- mehanizmi proti kloniranju,
- pristopom z **varnostnim čipom** oziroma ***Secure Element*,**
- revizijskimi zapisi,
- mehanizmi za izredno zaklepanje in obnovo sistema.

I.7 Realni scenariji uporabe

Za operativno sprejemljivost je nujno, da sistem ne ostane zgolj abstrakten koncept, temveč da vsebuje jasne scenarije realne uporabe.

Takšni scenariji bi morali vključevati vsaj:

- primer pogrešanega otroka,
- primer suma nezakonite posvojitve,
- primer preverjanja sorodstva v zakonsko dopustnem postopku,
- primer fizičnega sprožilca za nujne primere,
- primer sodno odobrene identifikacije v posebej občutljivem primeru.

Šele konkretni scenariji omogočajo presojo:

- sorazmernosti,
- pravne dopustnosti,
- tehnične izvedljivosti,
- operativne smiselnosti.

I.8 Financiranje in upravljanje

Za vsak resen projekt je treba že v pobudi odpreti tudi vprašanje:

- kdo sistem financira,
- kdo upravlja infrastrukturo,
- kdo nosi odgovornost,
- kdo izvaja nadzor,
- kdo pokriva stroške certificiranja,
- kdo zagotavlja dolgoročno vzdrževanje.

Brez odgovora na ta vprašanja noben sistem ne more preiti iz ravni ideje v raven dejanske institucionalne obravnave.

PRILOGA II - DODATNA VARNOSTNA DOPOLNITEV: THREAT MODEL, VARNOSTNA ARHITEKTURA IN CERTIFIKACIJSKA USMERITEV

II.1 Osnovna varnostna premisa

Vsak sistem je teoretično mogoče napasti. Vendar je bistvena razlika med sistemi v tem, kako težko jih je napasti, koliko škode lahko napad povzroči in ali arhitektura že v osnovi zmanjšuje sistemska tveganja.

QEI sistem je lahko bistveno bolj odporen od klasičnih centraliziranih modelov, če je pravilno zasnovan, ker:

- nima centralne baze občutljivih podatkov,
- uporablja fragmentacijo,
- uporablja lokalno pretvorbo,
- uporablja kriptografske mehanizme,
- omogoča ločeno hrambo različnih slojev sistema.

II.2 Glavne površine napada

Napadalec lahko cilja zlasti na naslednje ravni:

- uporabnika,
- fizični token,
- uporabniško napravo,
- komunikacijo,
- certifikacijski ali institucionalni sloj,
- postopke obnove in preklica,
- socialni inženiring.

Največja realna tveganja niso nujno v matematični kriptografiji, temveč v:

- človeški napaki,
- kraji fizične naprave,
- zavajanju uporabnika,
- neustreznem upravljanju ključev,
- notranjih zlorabah.

II.3 Tipični napadi in predlagane zaščite

a) Kraja tokena

Najbolj realističen scenarij napada je fizična kraja naprave ali nosilca.

Predlagane zaščite:

- zaščita s PIN-kodo,
- časovna zakasnitev po napačnih poskusih,
- možnost takojšnje deaktivacije,
- varnostni čip (*Secure Element*),
- omejena funkcionalnost brez dodatnega faktorja.

b) Socialni inženiring

Napad je pogosto usmerjen v uporabnika, ne v sistem.

Predlagane zaščite:

- večstopenjska potrditev,
- jasna opozorila uporabniku,
- obvestila o uporabi,
- izobraževanje uporabnikov,
- izredno zaklepanje (*emergency lock*).

c) Napad na napravo

Napadalec lahko cilja telefon, računalnik ali drugo napravo.

Predlagane zaščite:

- *Trusted Execution Environment (**TEE**)*,
- *Secure Enclave*,
- izolacija ključev,
- prepoved izvoza občutljivega materiala,
- podpisovanje samo znotraj varnega modula.

d) Napad na komunikacijo

Možni so napadi s posrednikom oziroma prestrezanje zahtevkov.

Predlagane zaščite:

- šifriranje od konca do konca,
- podpisani zahtevki,
- mehanizem *challenge-response*,
- preverjanje integritete zahtevkov.

e) Napad na institucije

Napad lahko cilja certifikacijski ali podpisni organ.

Predlagane zaščite:

- brez hrambe surovih biometričnih podatkov,
- stroga ločitev funkcij,
- revizijska sled,
- večnivojski nadzor,
- redni varnostni pregledi.

II.4 Slojna varnostna arhitektura

Priporočena zasnova sistema mora slediti načelu **večplastne obrambe (*defense-in-depth*)**.

Layer 1 - Device Security

- varnostni čip (*Secure Element*),
- zaščita pred posegi v napravo (*anti-tamper*),
- šifrirana hramba podatkov.

Layer 2 - Crypto Layer

- zgoščevanje oziroma transformacija biometrije,
- digitalni podpisi,
- izolacija ključev,
- HKDF oziroma primerljivi postopki derivacije ključev.

Layer 3 - Communication Layer

- šifriranje od konca do konca,
- podpisani zahtevki,
- preverjanje integritete.

Layer 4 - Policy Layer

- družinski nadzor,
- prilagodljiv dostop,
- pravna pravila dostopa,
- sodni oziroma institucionalni pogoji aktivacije.

Layer 5 - Emergency Layer

- ERAP,
- izredno zaklepanje (*emergency lock*),
- obnova sistema (*recovery*),
- preklic oziroma razveljavitev (*revocation*).

Ključna varnostna ideja je, da mora napadalec hkrati prebiti več slojev sistema in ne zgolj ene same točke.

II.5 Certifikacijska in standardizacijska usmeritev

Če bo predlagani sistem napredoval v formalni razvojni program ali pilotno izvedbo, bi moral biti usklajen z mednarodno priznanimi standardi in regulativnimi okviri, ki jih sprejemajo javni organi, Evropska unija in institucionalni deležniki.

Med ključne usmeritve sodijo zlasti:

- **ISO/IEC 27001** - upravljanje informacijske varnosti,
- **FIDO2** - prijava brez gesla in strojna avtentikacija,

- **Common Criteria EAL5+** ali primerljiv nivo - za varnostne naprave in varnostne čipe,
- **eIDAS / eIDAS 2.0** - okvir elektronske identitete v Evropski uniji,
- skladnost z **GDPR** in nacionalno zakonodajo.

II.6 Ključni zaključek varnostne dopolnitve

Največji izziv takšnega sistema ni zgolj tehnologija, temveč kombinacija:

- pravne skladnosti,
- certificiranja,
- institucionalnega zaupanja,
- jasnega upravljanja,
- dokazljive varnosti.

QEI sistem lahko predstavlja resen varnostni koncept le, če je od začetka zasnovan kot:

- pravno obramben,
- tehnično decentraliziran,
- operativno preverljiv,
- certificiran,
- revizijsko sledljiv.

PRILOGA III - OPERATIVNI OKVIR ZA NADALJNJO OBRAVNAVO POBUDE

Za učinkovito nadaljnjo obravnavo pobude je smiselno poudariti, da sama shema, osnovna ideja ali predstavitveni material še ne zadostujejo za institucionalno presojo. Za resno pravno, strokovno in upravno obravnavo je potreben strukturiran dokument, ki ga lahko razumejo in ocenijo:

- ministrstva,
- institucije Evropske unije,
- regulatorji,
- pravni strokovnjaki,
- tehnološki partnerji,
- nadzorni organi.

Zato je smiselno, da se nadaljnje delo usmeri v naslednje operativne korake.

III.1 Priprava enotnega formalnega dokumenta

Potrebna je priprava enotne, celovite in notranje usklajene različice pobude, ki vsebuje najmanj:

- naslov in identifikacijo pobude,
- izvršni povzetek (*Executive Summary*),
- jasno opredelitev problema,
- opis predlagane rešitve,
- pravni okvir,
- tehnični okvir,
- konkretne scenarije uporabe,
- varnostne mehanizme,
- predlog nadaljnjih korakov.

Tak dokument mora biti primeren za formalno predložitev pristojnim organom in ne sme ostati zgolj na ravni konceptualnega prikaza.

III.2 Pravna dopolnitev in validacija

Pred nadaljnjo uporabo dokumenta v komunikaciji z institucijami je priporočljivo dodatno pravno uskladiti in jasno opredeliti:

- pravne podlage po **6. členu GDPR**,
- pravne podlage po **9. členu GDPR**,
- razmerje med privolitvijo in javnim interesom,
- vprašanje upravljavca in obdelovalca,
- režim izbrisa, preklica in pravic posameznika,
- vprašanje sodnega nadzora,
- razmerje do **eIDAS** in morebitnih prihodnjih evropskih okvirov.

Takšna pravna validacija bi bistveno povečala resnost in verodostojnost pobude.

III.3 Vsebinska koncentracija osrednjega namena

Za institucionalno sprejemljivost je posebej pomembno, da pobuda tudi v nadaljnjih fazah ostane vsebinsko osredotočena. Jedro dokumenta mora ostati jasno in razumljivo:

- zaščita otrok,
- identifikacija v izjemnih in posebej občutljivih primerih,
- odsotnost centralne baze podatkov,
- stroga pravna omejitev uporabe,
- visoka raven varstva zasebnosti.

Dodatne funkcionalnosti lahko ostanejo kot možne prihodnje razširitve, vendar ne smejo zamegliti osnovnega cilja pobude.

III.4 Določitev pristojnih naslovnikov

Za nadaljnjo obravnavo pobude je pomembno, da se dokument predloži jasno določenim institucijam in ne nedoločno ali splošno. Med potencialno pristojne naslovnike sodijo zlasti:

- **Evropska komisija - Generalni direktorat za pravosodje in varstvo potrošnikov (DG JUST),**
- **Evropska komisija - Generalni direktorat za migracije in notranje zadeve (DG HOME),**
- **Ministrstvo za notranje zadeve Republike Slovenije,**
- **Ministrstvo za pravosodje Republike Slovenije,**
- **Informacijski pooblaščenec Republike Slovenije,**
- **Varuh človekovih pravic Republike Slovenije,**
- **pristojni odbori Državnega zbora Republike Slovenije,**
- drugi pristojni organi glede na vsebino posamezne faze pobude.

Jasna določitev naslovnikov prispeva k večji procesni resnosti in boljši usmerjenosti nadaljnje komunikacije.

III.5 Predložitev pobude kot uradnega dokumenta

Pobuda naj se pristojnim organom predloži kot enoten, strukturiran ter pravno in tehnično usklajen dokument.

Nadaljnja komunikacija naj temelji na enotni različici besedila, ki jasno opredeljuje:

- namen pobude,
- pravni okvir,
- tehnično zasnovo,
- varovalke pred zlorabami,
- institucionalni pomen,
- predlagane nadaljnje korake.

Takšen pristop je bistveno primernejši od nepovezanega ali večkrat spreminjajočega se predstavljanja posameznih delov ideje.

III.6 Zaključna operativna usmeritev

Ključni naslednji korak ni zgolj nadaljnje dopolnjevanje ideje, temveč njena stabilizacija v obliki dokumenta, ki je dovolj jasen, celovit in strokovno utemeljen, da ga je mogoče predložiti v formalno obravnavo.

Z operativnega vidika je zato najbolj smiselno:

- pripraviti končno usklajeno različico pobude,
- opraviti osnovno pravno in tehnično validacijo,
- določiti prve institucionalne naslovnike,
- dokument predložiti kot uradno pobudo za začetek strokovne in javne razprave.

Takšen pristop zagotavlja strukturirano podlago za nadaljnji dialog z nacionalnimi organi, institucijami Evropske unije, akademsko skupnostjo in drugimi ustreznimi deležniki, hkrati pa ohranja temeljne cilje pobude, njeno pravno skladnost in tehnično celovitost.

INŠTITUT 1. APRIL

Raziskave • Inovacije • Napredne tehnologije

REPUBLIKA SLOVENIJA
VLADA REPUBLIKE SLOVENIJE

QEI HUMANITARNI SISTEM IDENTITETE IN POMOČI (QHIAS)

DIGITALNA IDENTITETA ZA DOSTOP DO HUMANITARNE POMOČI ZA BEGUNCE, MIGRANTE IN DRUGE RANLJIVE SKUPINE

RAZISKOVALNI PROJEKT PREDLAGAN ZA REPUBLIKO SLOVENIJO IN EVROPSKO UNIJO – ZA VARNO, HUMANITARNO IN DIGITALNO EVROPO

QHIAS je varen sistem digitalne identitete in humanitarne pomoči, zasnovan z namenom omogočanja dostopa do osnovnih storitev, pomoči in zaščite brez centralnega shranjevanja biometričnih podatkov.



KLJUČNE PREDNOSTI:

- Varna identifikacija brez shranjevanja biometričnih podatkov
- Dostop do humanitarne pomoči in storitev
- Preprečevanje zlorab ter ustvarjanje dvojnih identitet
- Zaščita otrok brez spremstva
- Skladnost z GDPR in človekovimi pravicami
- Pregledna in sledljiva poraba javnih sredstev

DIGITALNA DENARNICA

DOSTOP DO DENARNIH SREDSTEV, POMOČI IN STORITEV

Varna distribucija finančnih sredstev in bonov za hrano, nastanitev, zdravstvenp, oskrbo, izobraževanje in še več.

HUMANITARNA POMOČ

HRANA, NASTANITEV, ZDRAVSTVO, IZOBRAŽEVANJE

Hitro in učinkovito zagotavljanje pomoči v kriznih razmerah in ob humanitarnih nesrečah.

ZAŠČITA OTROK BREZ SPREMSTVA

IDENTIFIKACIJA IN ZAŠČITA NAJBOLJ RANLJIVIH

Posebni mehanizmi za identifikacijo in zaščito otrok brez spremstva ter ločenih od družine.

ZASEBNOST IN VARNOST

ZAŠČITA ZASEBNOSTI BREZ MNOŽIČNEGA NADZORA IN ZLORAB

Močna šifriranje, omejitev namena obdelave in neodvisen nadzor zagotavljajo varnost in zasebnost.

IDENTITETA. ZAŠČITA. POMOČ. DOSTOJANSTVO.

ČLOVEŠKO DOSTOJANSTVO · ZASEBNOST PO NAČRTU · VARNOST · TRANSPARENTNOST · ODGOVORNOST · SOLIDARNOST

GDPR SKLADNO

Projekt je skladen z GDPR, Listino EU o temeljnih pravicah ter mednarodnimi humanitarnimi standardi.

Predlagatelj: Inštitut 1. april | Izola, Slovenija | 2026 | institut1april.com

PRILOGA IV - SISTEM ZA HUMANITARNO IDENTITETO IN POMOČ QEI (QHIAS)

DODATNA MOŽNA UPORABA TEHNOLOGIJE QEI ZA ZAŠČITO BEGUNCEV, MIGRANTOV IN DRUGIH RANLJIVIH SKUPIN

IV.1 Uvod

Evropska unija se v zadnjih desetletjih sooča z vse večjimi migracijskimi tokovi, humanitarnimi krizami, vojnami, naravnimi nesrečami in primeri trgovine z ljudmi.

Posebej ranljive skupine predstavljajo:

- otroci brez spremstva,
- osebe brez osebnih dokumentov,
- begunci,
- migranti,
- žrtve trgovine z ljudmi,
- osebe, ki zaradi vojn ali katastrof izgubijo možnost dokazovanja svoje identitete.

Namen te priloge je predstaviti možno uporabo sistema **QHIAS (*QEI Humanitarian Identity & Aid System*)** kot okvira za humanitarno identiteto, ki bi lahko prispeval k varstvu temeljnih pravic, olajšal varno in zanesljivo preverjanje identitete ter podprl pregledno zagotavljanje humanitarne pomoči, hkrati pa v celoti spoštoval pravico posameznika do zasebnosti in veljavna pravna varovala.

IV.2 Namen sistema

Sistem **QHIAS (*QEI Humanitarian Identity & Aid System*)** je zamišljen kot prostovoljen, zasebnostno usmerjen in tehnološko napreden sistem za podporo humanitarnim programom.

Njegovi cilji vključujejo:

- zaščito otrok brez spremstva,
- zaščito beguncev in migrantov,
- preprečevanje trgovine z ljudmi,
- preprečevanje kraje identitete,
- zmanjševanje zlorab humanitarnih sistemov,
- hitrejšo identifikacijo oseb brez dokumentov,
- učinkovitejši dostop do socialnih in zdravstvenih storitev,
- bolj transparentno upravljanje humanitarne pomoči.

IV.3 Humanitarna digitalna identiteta

Vsak upravičenec bi lahko prejel:

- **QEI identifikacijski ključek,**
- **NFC identifikacijsko kartico,**

- **QR identifikator,**
- **digitalno identiteto,**
- **osebni varnostni PIN.**

Identiteta temelji na kriptografsko zaščitenem QEI tokenu in ne vsebuje surovih biometričnih podatkov.

Sistem ne vzpostavlja centralne baze biometrije in ne omogoča množičnega nadzora prebivalstva.

Dostop do identitete je mogoč izključno v okviru zakonodaje, določenih postopkov in ustreznega nadzora.

IV.4 Digitalna humanitarna denarnica

Okvir QHIAS lahko vključuje humanitarno digitalno denarnico, zasnovano za podporo varnemu, preglednemu in odgovornemu zagotavljanju humanitarne pomoči.

Njena uporaba bi lahko omogočala:

- prehranske bone,
- humanitarne transferje,
- socialno pomoč,
- dostop do zdravstvenih storitev,
- izobraževalne programe,
- pomoč pri nastanitvi,
- nujno pomoč ob krizah.

Sredstva lahko zagotavljajo:

- Evropska unija,
- države članice,
- mednarodne organizacije,
- humanitarne organizacije,
- javni programi pomoči.

Sistem omogoča sledljivost javnih sredstev in zmanjšuje možnost zlorab.

IV.5 Zaščita otrok brez spremstva

Posebna pozornost je namenjena zaščiti otrok brez spremstva, ki so med najbolj ranljivimi skupinami v humanitarnih in migracijskih kontekstih.

Sistem lahko pomaga pri:

- hitrejši identifikaciji otroka,
- zaščiti pred trgovino z otroki,
- preprečevanju nezakonitih posvojitev,
- zaščiti pred izkoriščanjem,
- združevanju družin,
- zaščiti otrok v begunskih centrih.

Namen predlaganega sistema ni spremljanje ali sledenje otrok, temveč krepitev njihove zaščite, varovanje njihovih pravic ter podpora pristojnim organom in humanitarnim organizacijam pri delovanju v najboljšem interesu otroka, v skladu z veljavnimi pravnimi standardi in standardi človekovih pravic.

IV.6 Preprečevanje trgovine z ljudmi

Trgovina z ljudmi ostaja ena najresnejših groženj ranljivim posameznikom, zlasti otrokom, beguncem, migrantom in drugim osebam, ki jim grozi izkoriščanje.

Predlagani okvir **QHIAS** lahko služi kot dopolnilni zaščitni mehanizem za podporo odkrivanju in preprečevanju:

- trgovine z ljudmi,
- spolnega izkoriščanja,
- prisilnega dela,
- organiziranega kriminala,
- nezakonitih migracijskih mrež.

Predlagani sistem ni namenjen nadomestitvi postopkov kazenskega pregona ali sodnih preiskav. Namesto tega je zasnovan tako, da dopolnjuje obstoječe pravne in institucionalne mehanizme s podporo varnemu preverjanju identitete v strogo opredeljenih, zakonsko dovoljenih okoliščinah in v popolnem skladu z veljavnimi zakoni in temeljnimi pravicami.

IV.7 Pravne in etične varovalke

Predlagani okvir QHIAS bi moral temeljiti na naslednjih načelih:

- spoštovanju človekovih pravic,
- spoštovanju GDPR,
- načelu ***Privacy by Design***,
- načelu ***Data Minimization***,
- načelu ***Purpose Limitation***,
- prepovedi diskriminacije,
- prepovedi politične uporabe,
- prepovedi množičnega nadzora,
- popolni revizijski sledljivosti.

Sistem ne sme omogočati:

- političnega profiliranja,
- verskega profiliranja,
- spremljanja lokacije posameznika,
- komercialne uporabe podatkov,
- avtomatiziranega odločanja brez človekovega nadzora.

IV.8 Pametna distribucija pomoči

V prihodnosti lahko sistem omogoča:

- hitrejšo distribucijo pomoči,
- preprečevanje dvojnih izplačil,
- zmanjšanje administrativnih stroškov,
- boljši nadzor nad porabo javnih sredstev,
- učinkovitejšo pomoč ob naravnih nesrečah,
- učinkovitejšo pomoč ob vojnah in krizah.

Vsaka prihodnja izvedba teh zmogljivosti bi morala ostati podvržena veljavnim pravnim varovalkam, ustreznemu institucionalnemu nadzoru ter temeljnim načelom preglednosti, sorazmernosti in varstva temeljnih pravic.

IV.9 Digitalna identiteta za osebe brez dokumentov

Mnogi posamezniki izgubijo svoje osebne dokumente zaradi oboroženih spopadov, naravnih nesreč, humanitarnih kriz ali prisilnega razseljevanja.

Predlagani okvir **QHIAS** bi lahko podprl izdajo začasne humanitarne digitalne identitete za lažji dostop do:

- osnovnega zdravstvenega varstva,
- humanitarne pomoči,
- socialnih programov,
- izobraževanja,
- pravne pomoči.

Takšna humanitarna digitalna identiteta ni namenjena nadomestitvi državljanstva, narodnosti, zakonitega prebivališča ali katerega koli drugega pravno priznanega civilnega statusa.

Namesto tega je zasnovana tako, da zagotavlja začasen in varen način dostopa do bistvenih storitev, medtem ko se posameznikova pravna identiteta ali status ugotavlja oziroma preverja v skladu z veljavnim nacionalnim pravom, pravom Evropske unije in mednarodnim pravom.

IV.10 Možna povezava z evropsko digitalno identiteto

Ker se evropski ekosistem digitalne identitete še naprej razvija, se lahko preuči interoperabilnost predlaganega okvira **QHIAS** z obstoječimi in prihodnjimi evropskimi infrastrukturami identitete.

Možna področja interoperabilnosti vključujejo:

- **eIDAS 2.0,**
- **Evropsko denarnico za digitalno identiteto (EUDI denarnica),**
- **decentralizirane identifikatorje (DID),**
- **preverljive poverilnice (VC).**

Takšna povezava mora vedno spoštovati:

- nacionalne ustavne okvire,
- zakonodajo Evropske unije,
- veljavno zakonodajo o varstvu podatkov in zasebnosti,
- načela nujnosti, sorazmernosti in omejitve namena.

Vsako takšno interoperabilnost bi bilo treba upoštevati le, če podpira humanitarne cilje sistema in ne ogroža zasebnosti, varnosti ali temeljnih pravic zadevnih posameznikov.

IV.11 Pilotni projekt Evropske unije

Za oceno izvedljivosti in potencialnih koristi predlaganega okvira QHIAS v nadzorovanem in zakonsko skladnem okolju se lahko razmisli o prostovoljnem pilotnem projektu.

Možni partnerji:

- **Evropska komisija,**
- **UNICEF,**
- **Visoki komisar Združenih narodov za begunce (UNHCR),**
- **Agencija Evropske unije za azil (EUAA),**
- **Evropska agencija za mejno in obalno stražo (Frontex),**
- države članice Evropske unije.

Cilji pilotnega projekta bi lahko vključevali:

- oceno tehnične izvedljivosti predlaganega okvira,
- oceno skladnosti z veljavnimi pravnimi in regulativnimi zahtevami,
- oceno stroškov izvajanja in delovanja,
- oceno morebitnega vpliva na temeljne pravice in varstvo podatkov,
- oceno morebitnih koristi za zaščito ranljivih oseb, zlasti otrok, beguncev, migrantov in žrtev trgovine z ljudmi.

Vsak pilotni projekt bi moral potekati izključno na prostovoljni osnovi, pod neodvisnim nadzorom in v popolnem skladu z veljavno nacionalno zakonodajo, pravom Evropske unije in mednarodnimi standardi človekovih pravic.

IV.12 Sklep

Sistem za humanitarno identiteto in pomoč QEI (QHIAS) predstavlja potencialno humanitarno uporabo okvira QEI, zasnovanega za podporo zaščiti beguncev, migrantov, otrok brez spremstva in drugih ranljivih oseb.

Namen predlaganega sistema ni omogočiti nadzora prebivalstva, temveč okrepiti varstvo temeljnih pravic, izboljšati varno in pregledno zagotavljanje humanitarne pomoči, prispevati k preprečevanju trgovine z ljudmi in zagotoviti okvir digitalne identitete, ki ohranja zasebnost za humanitarne namene.

Vsako prihodnje obravnavanje, razvoj ali izvajanje predlaganega okvira bi moralo temeljiti na celoviti pravni, tehnični, etični in operativni oceni ter bi moralo biti v skladu z najvišjimi standardi varstva človekovih pravic, zasebnosti, varstva podatkov, varnosti in institucionalne odgovornosti.

Predlagani okvir bi bilo treba obravnavati kot osnovo za nadaljnjo strokovno razpravo in vrednotenje, ne pa kot predlog za takojšnjo izvedbo. Vsaka prihodnja uporaba bi morala biti predmet prostovoljnega sodelovanja, demokratičnega nadzora in popolne skladnosti z veljavnimi nacionalnimi pravnimi okviri, pravnimi okviri Evropske unije in mednarodnimi pravnimi okviri.

PRILOGA V - TEHNIČNA ARHITEKTURA IN PRIHODNJI RAZVOJNI MODEL SISTEMA QEI

DODATNA STROKOVNA DOPOLNITEV ZA NADALJNJI RAZVOJ DIGITALNE IDENTITETE, KRIPTOGRAFSKE AVTENTIKACIJE IN DECENTRALIZIRANIH IDENTITETNIH SISTEMOV

V.1 Namen priloge

Namen te priloge je predstaviti možne tehnične smernice za prihodnji razvoj ogrodja **QEI, kvantizirane šifrirane identitete**, in orisati možne implementacije napredne arhitekture digitalne identitete, ki združuje biometrijo, kriptografijo, decentralizirane tehnologije identitete in sodobne varnostne mehanizme.

Ta priloga ne predstavlja končne tehnične specifikacije. Namesto tega zagotavlja okvir za raziskave in razvoj, namenjen podpori nadaljnjega strokovnega ocenjevanja, tehničnega vrednotenja, pilotnih projektov in morebitne prihodnje implementacije na nacionalni, evropski ali mednarodni ravni.

V.2 Večfaktorski biometrični model

Predlagani okvir **QEI** temelji na konceptu kombiniranja več neodvisnih biometričnih dejavnikov za vzpostavitev visoke ravni zanesljivosti, varnosti in odpornosti.

Možni biometrični faktorji vključujejo:

- prstni odtis,
- obrazno biometrijo,
- glasovni vzorec,
- šarenico,
- geometrijo obraza,
- kožne markerje,
- znamenja,
- brazgotine,
- tatuje,
- druge dovoljene biometrične karakteristike,
- opcijsko transformirane STR-markerje.

Vsak biometrični dejavnik se pred kakršno koli kriptografsko obdelavo pretvori v standardizirano biometrično predlogo.

Predlagani okvir ne uporablja surovih biometričnih podatkov kot identifikatorja identitete. Namesto tega biometrični podatki služijo izključno kot lokalni vhod za ustvarjanje kriptografskega gradiva v skladu z načeli minimizacije podatkov, zasebnosti že pri vgradnji in varnega preverjanja identitete.

V.3 Stabilizacija biometričnih podatkov

Ker se biometrični zajemi med posameznimi poskusi preverjanja pristnosti naravno razlikujejo, predlagani okvir QEI vključuje dodatne stabilizacijske mehanizme za zagotavljanje dosledne in zanesljive kriptografske obdelave.

Ti mehanizmi lahko vključujejo:

- fuzzy ekstraktor,
- kode za popravljanje napak (ECC),
- metode kvantizacije,
- normalizacijo značilnosti,
- stabilizacijo predloge.

Primeri:

Tabela: Biometrični faktor in standardizirana predstavitev:

Biometrični faktor	**Standardizirana predstavitev**
Prstni odtis	Feature Vector
Obraz	Embedding Vector
Glas	Voice Embedding
Tatu	Texture Descriptor

Opomba: *Standardizirana predstavitev pomeni tehnični zapis biometrične značilnosti, ki ni enak surovemu biometričnemu podatku.*

Po postopku stabilizacije sistem iz posameznega biometričnega faktorja izpelje ustrezen kriptografski material, na primer:

K_FP

K_FACE

K_VOICE

K_BODY

Te vrednosti predstavljajo kriptografski material, izpeljan iz standardiziranih biometričnih predlog, in ne iz samih biometričnih podatkov.

Takšen pristop omogoča, da sistem iz naravno nekoliko različnih biometričnih zajemov ustvari enak oziroma dovolj skladen kriptografski rezultat za nadaljnjo uporabo. S tem zagotavlja zanesljivo avtentikacijo, hkrati pa ohranja visoko raven zasebnosti in varnosti biometričnih informacij.

V.4 Generiranje kriptografske identitete

Končni kriptografski identifikacijski ključ nastane z združitvijo več med seboj neodvisnih biometričnih in varnostnih faktorjev.

Primer:

$$K\_FINAL = HKDF(K\_FP \,||\, K\_FACE \,||\, K\_BODY \,||\, SALT \,||\, CTX)$$

Pri tem:

- **K_FP** = kriptografski material, izpeljan iz prstnega odtisa,
- **K_FACE** = kriptografski material, izpeljan iz obrazne biometrije,
- **K_BODY** = kriptografski material, izpeljan iz telesnih markerjev, na primer znamenj, brazgotin ali tatujev,
- **SALT** = naključni varnostni parameter, ki zagotavlja enoličnost in odpornost proti vnaprej pripravljenim napadom,
- **CTX (Context)** = kontekst uporabe, vezan na določen namen ali okolje, ki preprečuje povezljivost rezultatov med različnimi sistemi ali primeri uporabe.

Takšen pristop omogoča, da končni kriptografski ključ ni odvisen od enega samega biometričnega faktorja, temveč predstavlja rezultat varne kombinacije več neodvisnih vhodov skupaj z dodatnimi kriptografskimi varnostnimi elementi.

Iz tako pridobljenega ključa se ustvari:

$$QEI\_TOKEN = SHA3\text{-}512(K\_FINAL \,||\, CTX)$$

QEI token:

- ne vsebuje osebnih podatkov,
- ne vsebuje biometrije,
- ne omogoča rekonstrukcije identitete,
- ne omogoča rekonstrukcije biometričnih podatkov,
- ne vsebuje zdravstvenih ali genetskih informacij.

QEI token služi izključno kot anonimiziran kriptografski identifikator in je namenjen zgolj preverjanju identitete v zakonsko dovoljenih in strogo nadzorovanih postopkih. Sam po sebi ne razkriva ali predstavlja identitete posameznika.

V.5 Lokalna obdelava in varni moduli

Vsi biometrični podatki se obdelujejo izključno lokalno.

Podprta okolja lahko vključujejo:

- **Trusted Execution Environment (TEE),**
- **Secure Enclave,**
- **Secure Element,**
- **StrongBox,**
- **Hardware Security Module (HSM),**
- druge certificirane varnostne module.

Biometrija nikoli ne zapusti naprave v surovi ali rekonstruabilni obliki.

Strežnik prejme zgolj:

- **QEI token**,
- javni ključ,
- kriptografsko podpisane rezultate.

Ta arhitektura znatno zmanjša tveganje kraje biometričnih podatkov, obsežnih kršitev podatkov in nepooblaščenega množičnega izkoriščanja, saj zagotavlja, da občutljivi biometrični podatki ostanejo omejeni na zaupanja vredna lokalna okolja za obdelavo.

V.6 Kriptografska avtentikacija

Sistem uporablja mehanizem ***Challenge-Response***.

Postopek:

1. strežnik pošlje kriptografski izziv,
2. naprava lokalno generira ali odklene **K_FINAL**,
3. naprava ustvari digitalni podpis,
4. strežnik preveri podpis.

Sistem nikoli ne pošilja:

- surove biometrije,
- biometričnih predlog,
- genetskih podatkov,
- osebnih podatkov.

Rezultat je:

- dostop odobren,
- dostop zavrnjen,
- zahteva dodatni faktor.

Takšna zasnova zagotavlja visoko stopnjo zasebnosti in varnosti.

V.7 Decentralizirana digitalna identiteta

Okvir **QEI** je zasnovan za podporo interoperabilnosti z decentraliziranimi ekosistemi digitalne identitete in sodobnimi standardi za preverjanje identitete ter izmenjavo digitalnih poverilnic.

Ilustrativni konceptualni tok:

Biometrija

↓

QEI

↓

Par ključev Ed25519

↓

Digitalna Identiteta W3C DID

Potencialna interoperabilnost vključuje:

- **W3C DID**, decentralizirane identifikatorje,
- **preverljive poverilnice (VC)**,
- **Fundacijo Hyperledger**,
- projekte digitalne identitete **fundacije Linux**,
- **eIDAS 2.0**,
- **Evropsko denarnico za digitalno identiteto (EUDI Wallet**).

Ta pristop omogoča vzpostavitev digitalne identitete brez zanašanja na gesla, fizične identifikacijske dokumente ali centralizirane baze podatkov.

Posameznik ostaja glavni upravljavec svoje digitalne identitete in ohranja nadzor nad uporabo in razkritjem svojih digitalnih poverilnic v skladu z veljavno zakonodajo in načeli zasebnosti.

V.8 Možni produkti in področja uporabe

Na podlagi sistema QEI je mogoče razviti več različnih rešitev.

QEI kartica

Pametna kartica z varnostnim elementom.

Možne uporabe:

- elektronska identiteta,
- zdravstveni sistemi,
- javna uprava,
- bančništvo.

QEI mobilna aplikacija

Mobilna aplikacija za digitalno identiteto brez uporabe gesel.

Primer uporabe:

Prepoznavanje obraza + prstni odtis = digitalna identiteta

QEI mejni sistem

Napredni sistem identifikacije na mejnih prehodih.

QEI humanitarni sistem

Digitalna identiteta za begunce, migrante in humanitarne programe.

QEI sistem za zaščito otrok

Zaščita otrok, pogrešanih oseb in preprečevanje trgovine z ljudmi.

QEI varni trezor

Zaščita:

- digitalnih sredstev,
- kripto denarnic,
- občutljivih dokumentov,
- poslovnih skrivnosti.

QEI sistem za državljane

Prihodnja digitalna identiteta za državljane.

QEI zdravstveni sistem

Varna identiteta za zdravstvene sisteme in zdravstveno dokumentacijo.

V.9 Upravljanje življenjskega cikla identitete

Ena ključnih prednosti ogrodja QEI je njegova sposobnost regeneracije kriptografskega identitetnega materiala brez potrebe po kakršni koli spremembi bioloških značilnosti posameznika.

Postopek:

- generira se nov **SALT**,
- določi se nov **CTX**,
- izvede se nova transformacija,
- ustvari se nov **QEI token**,
- stari identifikacijski material se deaktivira.

Ta pristop omogoča ogrodju, da obnovi varnost po izgubi, kraji ali ogrožanju kriptografskega gradiva, povezanega z identiteto, ne da bi pri tem potreboval nove biometrične značilnosti.

V primerjavi s konvencionalnimi biometričnimi sistemi za identifikacijo ta zmogljivost zagotavlja znatno varnostno prednost, saj podpira varno obnovo identitete, hkrati pa ohranja obstoječe biometrične značilnosti posameznika.

V.10 Varnostne prednosti arhitekture

Predlagana arhitektura **QEI** združuje več komplementarnih varnostnih mehanizmov, vključno z:

- večfaktorsko biometrijo,
- lokalno obdelavo,
- kriptografsko tokenizacijo,
- decentraliziranimi identitetami,
- možnostjo preklica in regeneracije,
- odsotnostjo centralne baze biometrije,
- visoko stopnjo zasebnosti.

Arhitektura je zasnovana v skladu z naslednjimi mednarodno priznanimi načeli varnosti in zasebnosti:

- ***Privacy by Design*** - varstvo zasebnosti že po zasnovi sistema,
- ***Privacy by Default*** - varstvo zasebnosti kot privzeta nastavitev,
- ***Data Minimization*** - načelo najmanjšega obsega podatkov,
- ***Purpose Limitation*** - načelo omejitve namena obdelave,
- ***Security by Design*** - varnost že po zasnovi sistema,
- ***Zero Trust Principles*** - načela arhitekture ničelnega zaupanja.

Ta arhitekturni model zmanjšuje tveganja, povezana s centraliziranimi podatkovnimi repozitoriji, krepi odpornost proti kibernetskim napadom in izboljšuje zaščito osebnih ter biometričnih podatkov z decentralizirano obdelavo in kriptografskimi zaščitnimi ukrepi.

V.11 Raziskovalni in razvojni potencial

Predlagani okvir **QEI** ima potencial za nadaljnje raziskave in razvoj na širokem spektru področij uporabe, vključno s področji:

- digitalne identitete,
- zaščite otrok,
- humanitarnih programov,
- javne uprave,
- zdravstva,
- bančništva,
- kritične infrastrukture,
- kibernetske varnosti,
- decentraliziranih identitet,
- digitalnih denarnic,
- prihodnjih evropskih identitetnih sistemov.

Možne raziskovalne poti vključujejo:

- umetno inteligenco za preverjanje identitete,
- postkvantno kriptografijo,
- evropske digitalne denarnice,
- interoperabilnost med državami,
- zaščito kritične infrastrukture,
- varne identitete za internet stvari (IoT).

Predlagani okvir bi se lahko nadalje razvil z evropskimi programi za raziskave, inovacije in digitalno preobrazbo, vključno s skupnimi pobudami, ki vključujejo javne organe, raziskovalne ustanove, univerze, industrijske partnerje in institucije Evropske unije.

V.12 Zaključek

Ključna inovacija sistema QEI ni posamezen biometrični faktor, temveč kombinacija:

- več neodvisnih biometričnih dejavnikov,
- tehnologije ***Fuzzy Extractor***,
- lokalne obdelave znotraj zaupanja vrednega izvajalnega okolja ***Trusted Execution Environment (TEE)*** ali enakovrednega varnega izvajalnega okolja,
- kriptografske tokenizacije,
- regeneracije identitete s parametri **SALT** in **CTX**,
- decentraliziranih digitalnih identitet,
- sodobnih kriptografskih mehanizmov.

Takšna arhitektura predstavlja možno osnovo za prihodnje generacije digitalnih identitet, ki združujejo visoko stopnjo varnosti, zasebnosti, interoperabilnosti in uporabnosti ter lahko prispevajo k razvoju varnejše digitalne družbe v Evropski uniji in širše.



Inštitut I.april ™

e: info@institut1april.com
w: institut1april.com

QEI POBUDA

ZA VARNEJŠO, PRAVIČNEJŠO IN ČLOVEKU USMERJENO PRIHODNOST



NAŠA VIZIJA

Ustvariti svet, v katerem je vsak posameznik varno prepoznan, zaščiten in obravnavan dostojanstveno – ne glede na starost, narodnost, poreklo ali okoliščine.

NAŠE POSLANSTVO

Z inovativnim sistemom Quantized Encrypted Identity (QEI) podpiramo zaščito otrok, beguncev, migrantov in vseh ranljivih skupin ter prispevamo k preprečevanju trgovine z ljudmi, krepitvi človekovih pravic in učinkovitejši humanitarni pomoči po vsem svetu.

NAŠE VREDNOTE

- Spoštovanje človekovih pravic in dostojanstva
- Zasebnost in varstvo osebnih podatkov
- Anonimizacija in minimalizacija podatkov
- Transparentnost in pravna omejenost
- Inovativnost in tehnološka odličnost
- Solidarnost in humanost

QEI – IDENTITETA PRIHODNOSTI
ZA LJUDI. ZA DRUŽBO. ZA SVET.

ZAŠČITA OTROK

Zaščita otrok brez spremstva, pogrešanih otrok in preprečevanje trgovine z otroki.

BEGUNCI IN MIGRANTI

Varna identiteta in dostop do storitev za begunce, migrante in druge ranljive skupine.

HUMANITARNA POMOČ

Učinkovita, poštena in pregledna distribucija pomoči v kriznih in humanitarnih situacijah.

VARNOST IN ZASEBNOST

Kriptografska zaščita, lokalna obdelava in brez shranjevanja surovih biometričnih podatkov.

GLOBALNA POVEZLJIVOST

Skladnost z evropskimi standardi (eIDAS 2.0, GDPR) in možnostjo globalne interoperabilnosti.

SKUPAJ GRADIMO SVET, V KATEREM JE VARNA IDENTITETA PRAVICA, NE PRIVILEGIJ.

Skladno z evropskimi vrednotami in pravnim okvirom Evropske unije.

Tehnologija, ki postavlja človeka v središče.

Partnerstvo za lepšo in varnejšo prihodnost nas vseh.

Inštitut 1.april™

RAZISKAVE • INOVACIJE • NAPREDNE TEHNOLOGIJE

IDENTITETA JE ZAUPANJE. ZAUPANJE JE PRIHODNOST.