L'IDENTITÀ È CONNESSIONE. LA CONNESSIONE È OPPORTUNITÀ.

ISTITUTO 1. APRILE

INIZIATIVA STRATEGICA

PER L'INTRODUZIONE DI UN SISTEMA BIOMETRICO AVANZATO
PER LA PROTEZIONE DEI BAMBINI (QEI)



PER LA SICUREZZA. PER LA GIUSTIZIA. PER IL FUTURO.

PER LE PERSONE. PER LA SOCIETÀ. PER IL MONDO.

Istituto 1.aprile®

RICERCHE • INNOVAZIONI • TECNOLOGIE AVANZATE

IZOLA, SLOVENIA | institut1april.com | 2026

INIZIATIVA QEI

L'IDENTITÀ È OPPORTUNITÀ.
PER LE PERSONE. PER LA SOCIETÀ. PER IL MONDO.

L'Identità Quantizzata Crittografata (QEI) è un sistema digitale di identità avanzato, aperto e sicuro, che combina biometria, crittografia e tecnologie di identità decentralizzate per proteggere i più vulnerabili e sostenere un futuro più giusto per tutti.



PROTEZIONE DEI BAMBINI
Ricerca dei bambini scomparsi, protezione contro rapimenti e prevenzione della tratta di esseri umani.

RIFUGIATI E MIGRANTI
Identità sicura per rifugiati, migranti e altri gruppi vulnerabili per garantire dignità e sicurezza.

AIUTO UMANITARIO
Distribuzione efficiente e trasparente degli aiuti a chi ne ha bisogno, da parte di organizzazioni umanitarie sul campo.

IDENTITÀ DIGITALE
Identità digitale avanzata senza documenti, senza biometria fisica e senza database centralizzati di dati sensibili.

SICUREZZA E SOVRANITÀ
Archiviazione dei dati locali in ambienti sicuri (TEE / Secure Enclave) e protezione crittografica di livello superiore.

DIRITTI UMANI
Promozione della dignità, dei diritti umani e dell'equità riducendo le discriminazioni e lo sfruttamento dei dati.

ADOZIONE GLOBALE
Interoperabilità con gli standard europei e internazionali (eIDAS 2.0, GDPR) per l'uso in tutto il mondo.

PARTENARIATI
Insieme costruiamo un mondo in cui l'identità digitale sicura è un diritto – non un privilegio.

QEI – TECNOLOGIE CHE CONNETTONO

BIOMETRIA AVANZATA
Combinazione di più fattori biometrici per un'elevata affidabilità e precisione.

PROTEZIONE CRITTOGRAFICA
Algoritmi crittografici avanzati per una trasformazione sicura e immodificabile dell'identità.

ARCHIVIAZIONE LOCALE SICURA
I dati biometrici non lasciano mai il dispositivo. La sicurezza è integrata nel sistema.

IDENTITÀ DECENTRALIZZATA
Gli utenti possiedono la propria identità. Nessuna autorità centrale, nessuna dipendenza.

RIGENERAZIONE DELL'IDENTITÀ
Possibilità di revoca e creazione di nuove identità senza compromettere dati biologici.

CONFORMITÀ ED ETICA
Conformità al GDPR, eIDAS 2.0 e agli standard etici più elevati.

IL NOSTRO IMPEGNO

DIGNITÀ — Ogni persona merita rispetto e riconoscimento.

SOLIDARIETÀ — Tecnologia al servizio dell'umanità.

GIUSTIZIA — Opportunità e diritti uguali per tutti.

INNOVAZIONE — Soluzioni avanzate per un mondo migliore.

SOSTENIBILITÀ — Per le generazioni future e per il nostro pianeta.

INSIEME COSTRUIAMO UN MONDO IN CUI L'IDENTITÀ È SICURA, SOVRANA E ACCESSIBILE PER TUTTI.

Istituto 1.aprile®

RICERCA • INNOVAZIONE • TECNOLOGIE AVANZATE

IZOLA, SLOVENIA | institut1april.com | 2026

I N D I C E

0. MOTIVAZIONE STRATEGICA DELL'INTERVENTO (PERCHÉ ORA) pagina **8**
0.1 RAPPRESENTAZIONE SEMPLIFICATA DEL FUNZIONAMENTO DEL SISTEMA 9

1. INTRODUZIONE **9**

2. CONTESTO E FINALITÀ DELL'INIZIATIVA **10**
2.1 Contesto 10
2.2 Finalità dell'iniziativa 11

3. PRINCIPI FONDAMENTALI DEL SISTEMA **11**
3.1 Principio della volontarietà 11
3.2 Principio della limitazione della finalità 11
3.3 Principio della minimizzazione dei dati 11
3.4 Principio della tokenizzazione irreversibile 12
3.5 Principio della separazione dei registri 12
3.6 Principio del controllo giudiziario e indipendente 12

4. QUADRO GIURIDICO ED ETICO **12**
4.1 Quadro costituzionale 12
4.2 Quadro giuridico europeo 12
4.3 Principi etici 12
4.4 Test di proporzionalità 13
4.5 Test giuridico di proporzionalità 13
4.5.1 Obiettivo legittimo 13
4.5.2 Necessità della misura 13
4.5.3 Intervento minimo 13
4.5.4 Proporzionalità in senso stretto 14
4.6 Definizione giuridica dell'utilizzo del campione STR trasformato 14
4.7 Divieto esplicito di abuso 14
4.8 Principio fondamentale della separazione dell'identità 15
4.9 Chiarimento giuridico: sfatare i miti sui sistemi biometrici 15
4.9.1 Il GDPR non vieta, ma disciplina rigorosamente 15
4.9.2 Differenza fondamentale: il sistema non utilizza il DNA come dato 16
4.9.3 Conformità al principio *Privacy by Design* 16
4.9.4 Base costituzionale: la tutela dei bambini come valore superiore 16
4.9.5 Il sistema come meccanismo eccezionale di protezione, non di controllo 16
4.9.6 Conclusione del chiarimento giuridico 17

5. POSSIBILE MODELLO DI IMPLEMENTAZIONE **17**
5.1 Modello di implementazione di base 17
5.2 Quadro istituzionale 17
5.3 Natura complementare del sistema 18
5.4 Gestione e soggetto responsabile del sistema 18

6. MODELLO DI ADESIONE VOLONTARIA **18**
6.1 Adesione volontaria degli adulti 18
6.2 Adesione volontaria dei minori 18
6.3 Possibilità volontaria alla nascita 19

7. QEI - TOKEN BIOMETRICO DI IDENTIFICAZIONE pagina **19**
7.1 Definizione 19
7.2 Caratteristiche principali 19
7.3 Cosa non deve contenere il QEI 19
7.4 Definizione giuridica del sistema QEI 20
7.5 QEI - Physical Emergency Trigger Suite (PET-S) 20
7.5.1 Logica comune (sistema unificato) 20
7.5.2 Chiavetta fisica QEI 20
7.5.3 PET-2: Carta di emergenza (Child ID) 21
7.5.4 PET-3: Panic Trigger (dispositivo) 23
7.5.5 Integrazione nel sistema 25

8. PROPOSTA DI ARCHITETTURA E MODELLO DEI DATI DEL SISTEMA QEI **25**
8.1 Architettura di base 25
8.2 Registri separati 26
8.3 Principio di funzionamento del sistema 26
8.4 Architettura del sistema definita giuridicamente 27

9. TRILOCK - MODELLO DI SICUREZZA A TRE FATTORI **27**
9.1 Struttura di base 27
9.2 Modello di utilizzo a soglie 27
9.3 Combinazione delle chiavi 28
9.4 Principale vantaggio del modello 28
9.5 Modalità di funzionamento del meccanismo chiave QEI 28
9.6 QEI ONE - Chiave di sicurezza unificata 29

10. CAMPIONE BIOMETRICO STR COME FATTORE AGGIUNTIVO **31**
10.1 Ruolo corretto della componente STR 31
10.2 Processo di elaborazione 31
10.3 Regole fondamentali 31
10.4 Vantaggio giuridico di questa progettazione 31

11. AUTENTICAZIONE CRITTOGRAFICA **32**
11.1 Principio *Challenge-Response* 32
11.2 Cosa il sistema non trasmette mai 32
11.3 Principio *Fail-safe* 32

12. ELABORAZIONE LOCALE E MODULI SICURI **32**
12.1 Elaborazione locale 32
12.2 Divieto di esportazione della biometria 33
12.3 LConservazione locale delle chiavi 33
12.4 Assenza di una banca dati biometrica centralizzata 33

13. INFORMAZIONE ALL'UTENTE E CONTROLLO DELL'UTILIZZO **33**
13.1 Principio di trasparenza dell'utilizzo 33
13.2 Notifica all'utente 33
13.3 Audit e responsabilità 34

14. REVOCA E GESTIONE DEL CICLO DI VITA DELL'IDENTITÀ pagina **34**
14.1 Revocation 34
14.2 Vantaggio 34
14.3 Gestione dell'identità senza modificare le caratteristiche biologiche 34

15. REQUISITI NORMATIVI **35**
15.1 Requisiti normativi aggiuntivi 35

16. GARANZIE DI SICUREZZA E GIURIDICHE **35**

17. QUADRO FINANZIARIO E DI SVILUPPO **36**
17.1 Possibili fonti di finanziamento 36
17.2 Stima indicativa dei costi 36
17.3 Proprietà intellettuale e tutela brevettuale 36

18. PRESENTAZIONE PUBBLICA E INFORMAZIONE AL PUBBLICO **37**

19. PROPOSTA DEI PASSI SUCCESSIVI **38**
19.1 Orientamento strategico dei passi successivi 38
19.2 Proposta di progetto pilota 39

20. PROPOSTA UFFICIALE AL GOVERNO DELLA REPUBBLICA DI SLOVENIA **39**

21. ARGOMENTI GIURIDICI PER L'ULTERIORE DISCUSSIONE SPECIALISTICA **40**
21.1 Argomenti giuridici ampliati 40

22. PANORAMICA STATISTICA INDICATIVA E ALLEGATI **40**
22.1 Panoramica statistica indicativa 40
22.2 Rapimenti o sottrazioni di neonati dagli ospedali 42
22.3 Tratta globale di esseri umani - quota dei minori 42
22.4 Fonti del materiale di accompagnamento / note 43

23. CONCLUSIONE **45**

24. FONTI E BIBLIOGRAFIA **46**
24.1 Atti giuridici internazionali 46
24.2 Legislazione europea 46
24.3 Legislazione nazionale della Repubblica di Slovenia 46
24.4 Standard internazionali e linee guida specialistiche 46
24.5 Letteratura specialistica 47

25. GLOSSARIO DEI PRINCIPALI TERMINI, ACRONIMI E TERMINI STRANIERI **48**

ALLEGATO I - INTEGRAZIONE TECNICA AGGIUNTIVA:
ELEMENTI CHIAVE MANCANTI PER L'IMPLEMENTAZIONE REALE **52**
I.1 Root of Trust 52
I.2 Base giuridica (GDPR + eIDAS + quadro nazionale) 52
I.3 Gestione delle chiavi (Key Management) 53
I.4 Standard e interoperabilità 53
I.5 Flusso di verifica (Verification Flow) 54

I.6 Attacchi e abusi pagina 54
I.7 Scenari reali di utilizzo 54
I.8 Finanziamento e gestione 55

ALLEGATO II - INTEGRAZIONE AGGIUNTIVA SULLA SICUREZZA: THREAT MODEL, ARCHITETTURA DI SICUREZZA E ORIENTAMENTO ALLA CERTIFICAZIONE 56
II.1 Premessa fondamentale sulla sicurezza 56
II.2 Principali superfici di attacco 56
II.3 Attacchi tipici e misure di protezione proposte 56
II.4 Architettura di sicurezza a livelli 58
II.5 Orientamento alla certificazione e alla standardizzazione 58
II.6 Conclusione principale dell'integrazione sulla sicurezza 59

ALLEGATO III - QUADRO OPERATIVO PER L'ULTERIORE ESAME DELL'INIZIATIVA 60
III.1 Preparazione di un documento formale unitario 60
III.2 Integrazione giuridica e validazione 60
III.3 Concentrazione dei contenuti sulla finalità principale 61
III.4 Individuazione dei destinatari competenti 61
III.5 Presentazione dell'iniziativa come documento ufficiale 61
III.6 Orientamento operativo conclusivo 62

ALLEGATO IV - SISTEMA QEI PER L'IDENTITÀ E L'ASSISTENZA UMANITARIA (QHIAS) 64
IV.1 Introduzione 64
IV.2 Finalità del sistema 64
IV.3 Identità digitale umanitaria 64
IV.4 Portafoglio digitale umanitario 65
IV.5 Protezione dei minori non accompagnati 65
IV.6 Prevenzione della tratta di esseri umani 66
IV.7 Garanzie giuridiche ed etiche 66
IV.8 Distribuzione intelligente degli aiuti 66
IV.9 Identità digitale per le persone prive di documenti 67
IV.10 Possibile integrazione con l'identità digitale europea 67
IV.11 Progetto pilota dell'Unione europea 68
IV.12 Conclusione 68

ALLEGATO V - ARCHITETTURA TECNICA E MODELLO DI SVILUPPO FUTURO DEL SISTEMA QEI 70
V.1 Finalità dell'allegato 70
V.2 Modello biometrico multifattoriale 70
V.3 Stabilizzazione dei dati biometrici 71
V.4 Generazione dell'identità crittografica 72
V.5 Elaborazione locale e moduli sicuri 72
V.6 Autenticazione crittografica 73
V.7 Identità digitale decentralizzata 73
V.8 Possibili prodotti e ambiti di applicazione 74
V.9 Gestione del ciclo di vita dell'identità 75
V.10 Vantaggi di sicurezza dell'architettura 76
V.11 Potenziale di ricerca e sviluppo 76
V.12 Conclusione 77

RIASSUNTO

L'Istituto 1. aprile presenta un'iniziativa strategica per lo sviluppo di un sistema avanzato di identità digitale, destinato alla protezione dei bambini e di altri gruppi particolarmente vulnerabili.

La soluzione proposta introduce il sistema di identificazione biometrica **QEI (Quantized Encrypted Identity)**, basato su dati biometrici anonimizzati e trasformati in modo irreversibile. Il sistema non memorizza campioni biologici, dati genetici o dati biometrici grezzi, ma genera token crittografici di identificazione che consentono una verifica sicura dell'identità esclusivamente sulla base di un'adeguata base giuridica e sotto rigoroso controllo.

La soluzione è progettata in conformità ai principi di **privacy by design**, della minimizzazione dei dati, della limitazione delle finalità del trattamento e della separazione degli archivi, ed è conforme al quadro giuridico europeo, compreso il **Regolamento generale sulla protezione dei dati (GDPR)**, la **Carta dei diritti fondamentali dell'Unione europea** e altri standard pertinenti in materia di protezione dei dati personali.

Il sistema può contribuire in modo significativo alla ricerca dei bambini scomparsi, alla prevenzione della tratta di esseri umani, all'individuazione delle adozioni illegali e alla risoluzione di casi in cui l'identificazione con i metodi esistenti non è possibile o non è sufficientemente affidabile.

La soluzione proposta si basa su concetti tecnologici originali nei settori della biometria, della crittografia e dell'identità digitale, per i quali sono in corso procedure di tutela della proprietà intellettuale e di protezione brevettuale.

La costituzione dell'**Istituto 1. aprile** e l'ulteriore sviluppo del sistema **QEI** rappresentano un passo importante verso la realizzazione di un'identità digitale del futuro sicura, etica, tecnologicamente avanzata e rispettosa della privacy nella **Repubblica di Slovenia**, nell'**Unione europea** e nella più ampia comunità internazionale.

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

INIZIATIVA PER IL DIBATTITO PUBBLICO E PER LA PREPARAZIONE DELLA LEGISLAZIONE

BSISTEMA DI IDENTIFICAZIONE BIOMETRICA PER LA PROTEZIONE DEI BAMBINI (QEI)

Proponente:

Istituto 1. aprile
e: info@institut1april.com
w: institut1april.com

Versione 1.0 - Aprile 2026

0. MOTIVO STRATEGICO PER AGIRE (PERCHÉ ORA)

Negli ultimi anni, l'Unione europea e gli Stati membri si trovano ad affrontare sfide crescenti nel campo della protezione dei bambini, in particolare nel contesto di:

- migrazioni transfrontaliere,
- criminalità organizzata e tratta di esseri umani,
- adozioni illegali,
- abusi dell'identità digitale,
- sviluppo dell'intelligenza artificiale e delle tecnologie deepfake.

Gli attuali sistemi di identificazione si basano principalmente su registri amministrativi che non sono direttamente collegati all'identità biologica dell'individuo, il che, in casi eccezionali, può consentire la manipolazione o l'abuso dell'identità.

Allo stesso tempo, l'Unione europea sta sviluppando nuovi quadri per l'identità digitale (eIDAS 2.0), aprendo la possibilità di integrare meccanismi di identificazione avanzati e rispettosi della privacy.

Si pone quindi una domanda fondamentale:

Lo Stato e l'Unione europea possono sviluppare un sistema che:

- migliori la protezione dei bambini,
- prevenga le forme più gravi di abuso,
- funzioni senza una banca dati centrale,
- rispetti i più elevati standard di tutela della privacy?

La presente iniziativa rappresenta una risposta a questa domanda e propone che un tale sistema venga almeno esaminato sotto il profilo tecnico, giuridico e scientifico.

0.1 RAPPRESENTAZIONE SEMPLIFICATA DEL FUNZIONAMENTO DEL SISTEMA

Per facilitarne la comprensione, il funzionamento di base del sistema può essere riassunto in quattro fasi:

- Il bambino (e i genitori) aderiscono volontariamente al sistema.
- A partire da un insieme minimo di dati biometrici viene generato un token crittografico anonimizzato.
- In caso di incidente, viene verificata la corrispondenza tra i token.
- L'identità può essere rivelata esclusivamente sulla base di un'adeguata base giuridica e sotto appropriato controllo.

Il sistema:

- non conserva dati biometrici grezzi,
- non contiene una banca dati centrale delle identità,
- non consente una sorveglianza generalizzata,
- opera esclusivamente in casi eccezionali.

1. INTRODUZIONE

La presente iniziativa propone l'avvio di un dibattito tecnico e pubblico sulla possibilità di introdurre un sistema volontario di identificazione biometrica per la protezione dei bambini, basato sull'utilizzo di token crittografici anonimizzati di identificazione (**QEI**).

Lo scopo esclusivo del sistema proposto sarebbe:

- la ricerca dei bambini scomparsi,
- la prevenzione della tratta di minori,
- l'individuazione delle adozioni illegali,
- la verifica della parentela biologica nei casi di fondato sospetto di gravi reati commessi ai danni dei minori.

L'obiettivo dell'iniziativa è esaminare la possibilità di istituire un sistema giuridicamente rigorosamente limitato, tecnicamente sicuro e costituzionalmente proporzionato, che operi esclusivamente nell'interesse della protezione dei bambini, nel pieno rispetto di:

- della Costituzione della Repubblica di Slovenia,
- del diritto dell'Unione europea,
- delle norme sulla protezione dei dati personali,
- del principio di proporzionalità,
- del principio della minima interferenza possibile con i diritti dell’individuo.

Nonostante gli attuali sistemi di registrazione delle nascite e di identificazione delle persone, continuano a esistere casi in cui l'identità di un bambino non è verificabile in modo affidabile oppure è stata modificata illegalmente. Tali lacune possono rappresentare un grave rischio per la protezione dei bambini, in particolare nei casi di:

- tratta di esseri umani,
- adozioni illegali,
- reati transfrontalieri,
- controversie relative alla genitorialità,
- bambini scomparsi senza possibilità di un'identificazione affidabile.

I sistemi esistenti si basano generalmente su registri amministrativi che non sono direttamente collegati all'identità biologica. Il sistema **QEI** proposto apre un dibattito sulla possibilità di verificare l'identità sulla base di dati biometrici minimi, anonimizzati e trattati in modo irreversibile, senza conservare dati grezzi o dati biologici.

Nel sistema, i dati biometrici non rappresentano l'identità, ma servirebbero esclusivamente come meccanismo locale per sbloccare una chiave crittografica oppure per generare un token di identificazione irreversibile nell'ambito di procedure rigorosamente limitate.

I recenti casi transfrontalieri di tratta di minori, manipolazione dell'identità, adozioni illegali e l'aumento dei rischi di abuso digitale evidenziano la necessità di riflettere su nuovi meccanismi di protezione dei bambini rispettosi della privacy. Lo scopo di questa iniziativa è avviare in modo proattivo un dibattito tecnico e pubblico sulle possibili soluzioni, prima che tali rischi aumentino ulteriormente.

A causa della natura transfrontaliera della tratta di minori, delle adozioni illegali e dei casi di bambini scomparsi, l'iniziativa presenta una potenziale dimensione anche a livello dell'Unione europea. Un eventuale ulteriore sviluppo potrebbe pertanto esaminare in futuro anche l'interoperabilità con i quadri europei, nel rigoroso rispetto delle norme sulla protezione dei dati personali, del principio di sussidiarietà e dei limiti costituzionali.

Il modello tecnico presentato di seguito è illustrato a livello concettuale con l'obiettivo di dimostrare la fattibilità, i principi di sicurezza e le garanzie giuridiche. L'implementazione dettagliata sarebbe oggetto di successive analisi tecniche, giuridiche e scientifiche.

Se esiste una tecnologia che può salvare la vita anche di un solo bambino scomparso, è dovere dello Stato verificarne almeno la fattibilità costituzionale, giuridica e tecnica.

2. CONTESTO E OBIETTIVO DELL'INIZIATIVA

2.1 Contesto

L'iniziativa nasce dalla necessità di avviare un dibattito su un ulteriore meccanismo di protezione per i bambini, in particolare nei casi di:

- tratta di minori,
- schiavitù e sfruttamento sessuale dei minori,
- sottrazione di bambini alla nascita,
- adozioni illegali,
- errori sistemici nella registrazione della genitorialità,
- casi di bambini scomparsi senza una possibilità di identificazione affidabile.

Sebbene tali casi siano statisticamente relativamente rari, si tratta di reati estremamente gravi e delicati, nei quali anche un singolo caso può rappresentare una violazione eccezionalmente grave dei diritti umani e della dignità del bambino.

2.2 Obiettivo dell'iniziativa

L'obiettivo dell'iniziativa è aprire un dibattito tecnico, giuridico, scientifico ed etico sulla possibilità di istituire un sistema che:

- operi esclusivamente per la protezione dei bambini,
- sia volontario,
- utilizzi modelli biometrici minimi,
- non conservi campioni biologici né dati biometrici grezzi,
- consenta l'utilizzo esclusivamente sulla base di una rigorosa base giuridica,
- sia sottoposto a un controllo indipendente,
- impedisca qualsiasi estensione della finalità d'uso.

3. PRINCIPI FONDAMENTALI DEL SISTEMA

Il sistema proposto dovrebbe basarsi sui seguenti principi.

3.1 Principio della volontarietà

L'adesione al sistema sarebbe possibile esclusivamente sulla base di un consenso libero, informato ed esplicito.

3.2 Principio della limitazione della finalità

Il sistema potrebbe essere utilizzato esclusivamente per la protezione dei bambini, in particolare per:

- la ricerca dei bambini scomparsi,
- la prevenzione della tratta di minori,
- l'individuazione delle adozioni illegali,
- la verifica della parentela biologica nei casi previsti dalla legge.

L'utilizzo per altre finalità dovrebbe essere espressamente vietato, in particolare per:

- il perseguimento penale generale degli adulti,
- procedimenti fiscali,
- analisi sanitarie,
- finalità commerciali,
- sorveglianza generale della popolazione.

3.3 Principio della minimizzazione dei dati

Il sistema non dovrebbe conservare:

- campioni biologici dopo il trattamento,

- dati biometrici grezzi,
- l'intero patrimonio genetico,
- dati genetici sanitari,
- dati personali all'interno del token QEI.

3.4 Principio della tokenizzazione irreversibile

Il sistema utilizzerebbe esclusivamente modelli biometrici standardizzati dai quali verrebbero generati token crittografici di identificazione irreversibili.

3.5 Principio della separazione degli archivi

I dati identificativi, i modelli biometrici e i dati di audit dovrebbero essere conservati in modo rigorosamente separato, senza una banca dati centrale unica contenente dati sensibili.

3.6 Principio del controllo giudiziario e indipendente

L'accesso ai dati o l'avvio della procedura di identificazione dovrebbe essere possibile esclusivamente sulla base di:

- una base giuridica,
- un'ordinanza giudiziaria, ove richiesta,
- una rigorosa tracciabilità mediante audit,
- un controllo istituzionale indipendente.

4. QUADRO GIURIDICO ED ETICO

Il sistema proposto dovrebbe essere progettato in conformità ai seguenti principi giuridici ed etici.

4.1 Quadro costituzionale

- articolo della Costituzione della Repubblica di Slovenia - tutela del diritto alla privacy e dei diritti della personalità;
- articolo della Costituzione della Repubblica di Slovenia - speciale tutela dei bambini.

4.2 Quadro giuridico europeo

- Regolamento generale sulla protezione dei dati (GDPR), in particolare gli articoli 6 e 9;
- Carta dei diritti fondamentali dell'Unione europea - articoli 7 e 8;
- Convenzione europea dei diritti dell'uomo - articolo 8.

4.3 Principi etici

Il sistema proposto dovrebbe seguire i seguenti principi:

- privacy by design,
- privacy by default,

- proporzionalità,
- necessità,
- minimo intervento,
- tracciabilità,
- responsabilità,
- separazione tra i sistemi,
- divieto dell'uso secondario dei dati.

4.4 Test di proporzionalità

Qualsiasi futura disciplina legislativa dovrebbe superare un test di proporzionalità che comprenda:

- obiettivo legittimo - la protezione dei bambini;
- idoneità della misura;
- necessità della misura;
- minimo intervento possibile nei diritti dell'individuo.

4.5 Test giuridico di proporzionalità

Il sistema proposto è concepito in modo da superare il test di proporzionalità secondo la giurisprudenza costituzionale ed europea.

4.5.1 Obiettivo legittimo

La protezione dei bambini contro le forme più gravi di reato rappresenta un valore costituzionalmente tutelato ai sensi dell'articolo 56 della Costituzione della Repubblica di Slovenia e costituisce un obiettivo legittimo ai sensi del diritto dell'Unione europea e della Convenzione europea dei diritti dell'uomo.

4.5.2 Necessità della misura

Gli attuali sistemi amministrativi non consentono sempre un'identificazione affidabile nei casi di:

- adozioni illegali,
- tratta di minori,
- casi transfrontalieri privi di documentazione adeguata,
- controversie sulla genitorialità in circostanze particolarmente delicate.

Il sistema proposto rappresenta un meccanismo complementare destinato ai casi eccezionali in cui misure meno invasive non garantiscono la medesima efficacia.

4.5.3 Minimo intervento

Il sistema è progettato in modo da:

- non conservare dati biometrici o genetici nella loro forma grezza,
- utilizzare esclusivamente modelli trasformati, standardizzati e irreversibili,
- operare senza l'identificazione diretta della persona,

- non consentire la sorveglianza generale della popolazione,
- rivelare l'identità solo in presenza di condizioni giuridiche rigorosamente definite.

4.5.4 Proporzionalità in senso stretto

Le misure proposte sono rigorosamente limitate:

- alla protezione dei bambini,
- all'adesione volontaria,
- al controllo giudiziario o previsto dalla legge,
- ai casi eccezionali e particolarmente delicati.

Grazie a tali limitazioni, l'interferenza nei diritti è significativamente più contenuta rispetto ai tradizionali sistemi centralizzati di trattamento dei dati biometrici.

4.6 Definizione giuridica dell'utilizzo del modello STR trasformato

Nel sistema il DNA non viene utilizzato come dato identificativo o analitico, bensì esclusivamente come modello biometrico trasformato e irreversibile che:

- non consente l'identificazione diretta della persona,
- non contiene informazioni sanitarie o ereditarie,
- viene utilizzato esclusivamente come fattore di sicurezza aggiuntivo per un elevato livello di affidabilità.

Si applicano inoltre i seguenti principi:

- i dati grezzi del DNA non vengono mai conservati;
- il campione biologico viene distrutto immediatamente e in modo irreversibile dopo l'elaborazione;
- dalla rappresentazione trasformata non è possibile ricostruire il DNA originario.

Il modello STR trasformato:

- non viene utilizzato per l'autenticazione continua;
- non viene utilizzato come identificatore primario;
- non viene utilizzato per finalità sanitarie, diagnostiche o di ricerca.

Il sistema non utilizza il DNA a fini identificativi nel senso tradizionale, ma esclusivamente come fattore crittografico trasformato e irreversibile che non consente la divulgazione di informazioni genetiche o sanitarie.

4.7 Divieto esplicito di abuso

Il sistema non deve essere utilizzato per:

- la sorveglianza generale della popolazione,
- il perseguimento penale degli adulti al di fuori dell'ambito rigorosamente definito della protezione dei bambini,

- procedimenti fiscali o amministrativi,
- analisi sanitarie,
- ricerche genetiche,
- finalità commerciali,
- profilazione,
- processi decisionali automatizzati,
- sorveglianza di massa o uso secondario dei dati.

Qualsiasi estensione della finalità d'uso che vada oltre la protezione dei bambini nei casi previsti dalla legge deve essere espressamente vietata e punibile.

4.8 Principio fondamentale della separazione dell'identità

Il sistema, di per sé, non consente l'identificazione della persona. L'identificazione è possibile esclusivamente:

- in presenza di una corrispondenza confermata del token o di un altro risultato crittografico;
- quando sono soddisfatte le condizioni giuridiche previste;
- sulla base di un'ordinanza giudiziaria o di un'altra base giuridica prevista dalla legge;
- con la registrazione dell'accesso nel registro di audit.

In assenza di tali condizioni, l'identità non è accessibile.

4.9 Chiarimento giuridico: sfatare i miti sui sistemi biometrici

Nel dibattito pubblico è spesso diffusa l'errata convinzione che il quadro giuridico europeo, in particolare il Regolamento generale sulla protezione dei dati (GDPR), vieti completamente l'utilizzo dei dati biometrici e genetici. Tale interpretazione non è corretta.

4.9.1 Il GDPR non vieta, ma disciplina rigorosamente

L'articolo 9 del GDPR stabilisce che i dati biometrici e genetici costituiscono una categoria particolare di dati personali il cui trattamento è, in linea di principio, limitato, ma non assolutamente vietato.

Il trattamento è consentito quando esiste:

- il consenso esplicito dell'interessato;
- un importante interesse pubblico;
- un'adeguata base giuridica;
- una misura proporzionata e necessaria.

Il sistema proposto è progettato proprio su questi principi:

- piena volontarietà;
- rigorosa limitazione della finalità;
- minimizzazione dei dati;
- utilizzo esclusivamente nei casi eccezionali di protezione dei bambini.

4.9.2 Differenza fondamentale: il sistema non utilizza il DNA come dato

A differenza delle tradizionali banche dati biometriche o forensi, il modello proposto:

- non conserva il DNA;
- non conserva campioni biologici;
- non consente la ricostruzione dei dati genetici;
- non contiene informazioni sanitarie o altre informazioni sensibili.

Il DNA, o più precisamente la componente STR, viene utilizzato esclusivamente come input crittografico locale per generare una chiave irreversibile.

Ciò significa che il sistema:

- non crea una banca dati genetica;
- non consente l'identificazione senza una base giuridica;
- non costituisce un identificatore biologico permanente.

4.9.3 Conformità al principio di *privacy by design*

L'architettura proposta soddisfa fin dalla progettazione i principali requisiti del diritto europeo:

- trattamento dei dati esclusivamente in locale (TEE / Secure Enclave),
- archivi separati senza banca dati centrale,
- tokenizzazione irreversibile,
- divieto dell'uso secondario dei dati,
- completa tracciabilità degli accessi.

Una tale progettazione rappresenta addirittura uno standard di protezione dei dati superiore rispetto a quello adottato da molti sistemi esistenti.

4.9.4 Fondamento costituzionale: la protezione dei bambini come valore superiore

L'articolo 56 della Costituzione della Repubblica di Slovenia prevede una tutela speciale dei bambini. Ciò significa che lo Stato non è soltanto autorizzato, ma anche tenuto a valutare misure che possano migliorare la protezione dei bambini, purché siano:

- proporzionate,
- necessarie,
- conformi alla Costituzione.

4.9.5 Il sistema come meccanismo eccezionale di protezione, non di sorveglianza

È importante sottolineare che il sistema proposto:

- non è destinato all'identificazione generale della popolazione;

- non è destinato alla sorveglianza o al tracciamento;
- non può essere utilizzato senza una base giuridica;
- opera esclusivamente in casi eccezionali previsti dalla legge.

Si tratta di un meccanismo di protezione specializzato per i casi più gravi, nei quali i sistemi esistenti non sono sufficienti.

4.9.6 Conclusione del chiarimento giuridico

L'affermazione secondo cui l'ordinamento giuridico europeo vieterebbe integralmente un sistema di questo tipo non è corretta. Al contrario, con un'adeguata progettazione, appropriate garanzie e una base giuridica idonea, è possibile sviluppare una soluzione che:

- rispetti i diritti fondamentali,
- segua i principi della protezione dei dati,
- contribuisca efficacemente alla protezione dei bambini.

Pertanto, l'iniziativa non rappresenta una deroga all'attuale ordinamento giuridico, bensì un tentativo di svilupparlo ulteriormente nella direzione di una maggiore tutela delle persone più vulnerabili.

5. POSSIBILE MODELLO DI ATTUAZIONE

5.1 Modello di attuazione di base

Il modello proposto potrebbe basarsi sui seguenti elementi:

- conferimento volontario degli input biometrici dei genitori e dei bambini,
- trattamento esclusivamente di modelli biometrici minimi,
- creazione esclusiva di un token crittografico di identificazione,
- divieto di conservazione di dati biologici o di dati biometrici grezzi,
- attivazione delle procedure esclusivamente sulla base di un procedimento giuridicamente ammissibile,
- controllo istituzionale indipendente,
- sanzioni severe in caso di abuso.

5.2 Quadro istituzionale

Un possibile quadro istituzionale potrebbe includere:

- Ministero dell'Interno - gestione del sistema,
- Ministero della Salute - esecuzione del prelievo al momento dell'adesione,
- Polizia e servizi investigativi - utilizzo operativo nei casi previsti dalla legge,
- Garante per la protezione dei dati personali - controllo sulla protezione dei dati personali,
- organismo di controllo indipendente - audit del funzionamento del sistema,
- tribunali - decisione sull'ammissibilità dell'intervento e dell’accesso.

5.3 Natura complementare del sistema

Il sistema proposto non introduce una nuova forma di identificazione generale, ma rappresenta un ulteriore meccanismo di protezione rigorosamente limitato per i casi eccezionali in cui i sistemi esistenti risultano inefficaci.

Il sistema non è concepito come sostituto degli archivi esistenti, bensì come livello di protezione complementare destinato ai casi particolarmente delicati di protezione dei bambini.

5.4 Gestione e soggetto responsabile del sistema

Per l'attuazione operativa del sistema è fondamentale definire chiaramente il soggetto responsabile del progetto e la struttura di gestione.

Una possibile struttura di base potrebbe essere:

- istituzione capofila: lo Stato, ad esempio il Ministero dell'Interno, oppure un quadro europeo,
- soggetto tecnico responsabile e partner per lo sviluppo: Istituto 1. aprile,
- partner tecnologici: TBD (sviluppo, sicurezza, infrastruttura),
- organismo di controllo: istituzione indipendente, ad esempio il Garante per la protezione dei dati personali.

Tale suddivisione consente:

- una chiara attribuzione delle responsabilità,
- legittimità istituzionale,
- supporto tecnico,
- trasparenza della gestione.

6. MODELLO VOLONTARIO DI ADESIONE

6.1 Adesione volontaria degli adulti

Una persona adulta potrebbe aderire al sistema sulla base di un consenso scritto e informato.

Dovrebbe avere in qualsiasi momento il diritto di richiedere la cancellazione dei dati, qualora non sussista un'altra base giuridica per la loro conservazione.

6.2 Adesione volontaria dei bambini

L'adesione di un minore sarebbe possibile sulla base del consenso dei genitori o dei rappresentanti legali.

Al raggiungimento della maggiore età, la persona dovrebbe avere il diritto di:

- confermare la prosecuzione dell'adesione oppure
- richiedere la cancellazione dei dati.

6.3 Possibilità volontaria alla nascita

Alla nascita del bambino, ai genitori potrebbe essere offerta la possibilità di aderire al sistema.

La decisione dovrebbe essere:

- completamente volontaria,
- priva di qualsiasi conseguenza negativa in caso di rifiuto,
- attuata in conformità agli standard medici.

7. QEI - TOKEN DI IDENTIFICAZIONE BIOMETRICA

7.1 Definizione

Il **QEI (Quantized Encrypted Identity)** rappresenta un sistema di identificazione anonimizzato e protetto crittograficamente che genera un token di identificazione irreversibile a partire da modelli biometrici standardizzati.

Il QEI non costituisce un dato personale sotto forma di nome, numero identificativo personale o altro identificatore diretto, bensì un elemento tecnico di collegamento crittografico che consente la verifica della corrispondenza al ricorrere delle condizioni giuridiche previste.

7.2 Caratteristiche principali

Il nucleo del sistema sarebbe costituito da:

- modelli biometrici, non dati grezzi,
- un token QEI unificato,
- archivi separati,
- accesso a più livelli,
- tracciabilità tramite audit,
- tutela della privacy secondo il principio della *privacy by design*.

7.3 Cosa il QEI non deve contenere

Il token QEI non deve contenere:

- immagini grezze delle impronte digitali,
- fotografie del volto,
- l'intero patrimonio genetico,
- dati genetici sanitari,
- testo libero relativo alla persona,
- attributi politici, religiosi o altri dati sensibili,
- identificatori personali diretti.

7.4 Definizione giuridica del sistema QEI

Il QEI rappresenta un token di identificazione anonimo, generato crittograficamente a partire da modelli biometrici standardizzati, che:

- non contiene dati personali,
- non consente la ricostruzione dell'identità,
- non consente la ricostruzione dei dati biometrici,
- non contiene informazioni sanitarie, ereditarie o altre informazioni sensibili.

Il sistema garantisce:

- la completa separazione tra dati identificativi, modelli biometrici e registri di audit,
- l'utilizzo di funzioni crittografiche unidirezionali,
- la non correlabilità tra i sistemi,
- un controllo degli accessi giuridico e tecnico multilivello.

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

Per i casi in cui l'attivazione biometrica non sia possibile, non sia appropriata oppure non possa essere eseguita tempestivamente, si propone anche un sistema complementare di attivatori fisici senza utilizzo della biometria:

QEI - Physical Emergency Trigger Suite (PET-S)

(Tre modalità fisiche di attivazione senza utilizzo della biometria.)

7.5.1 Logica comune (sistema unificato)

Tutti e tre gli attivatori funzionano secondo la medesima logica:

- attivazione fisica,
- verifica crittografica,
- generazione della richiesta **Emergency Request (ER)**,
- attivazione del protocollo **ERAP**,
- senza utilizzo della biometria.

7.5.2 PET-1: Chiave fisica QEI

Forma:

- chiave USB-C oppure NFC,
- collegata al **Family Token**.



Attivazione:

- inserimento o avvicinamento della chiave,
- inserimento del PIN,
- il sistema genera una **Emergency Request (ER)**.

Sicurezza:

- chip di sicurezza (**Secure Element**),
- protezione contro la clonazione (**anti-clone**),
- collegamento al nucleo familiare.

Utilizzo:

- genitori,
- polizia, qualora disponga di un'adeguata base giuridica e dell'autorizzazione all’accesso.

7.5.3 PET-2: Carta di emergenza (Child ID)

Forma:

La carta contiene:

- un indicatore visivo dell'impronta digitale,
- un chip NFC,
- l'identificatore QEI (**QEI ID**).



Attivazione:

- una persona trova il bambino,
- scansiona la carta,
- il sistema verifica l'identificatore,
- invia un segnale all'autorità competente.

Sicurezza:

- esclusivamente un identificatore pseudonimizzato,
- nessun dato personale.

Utilizzo:

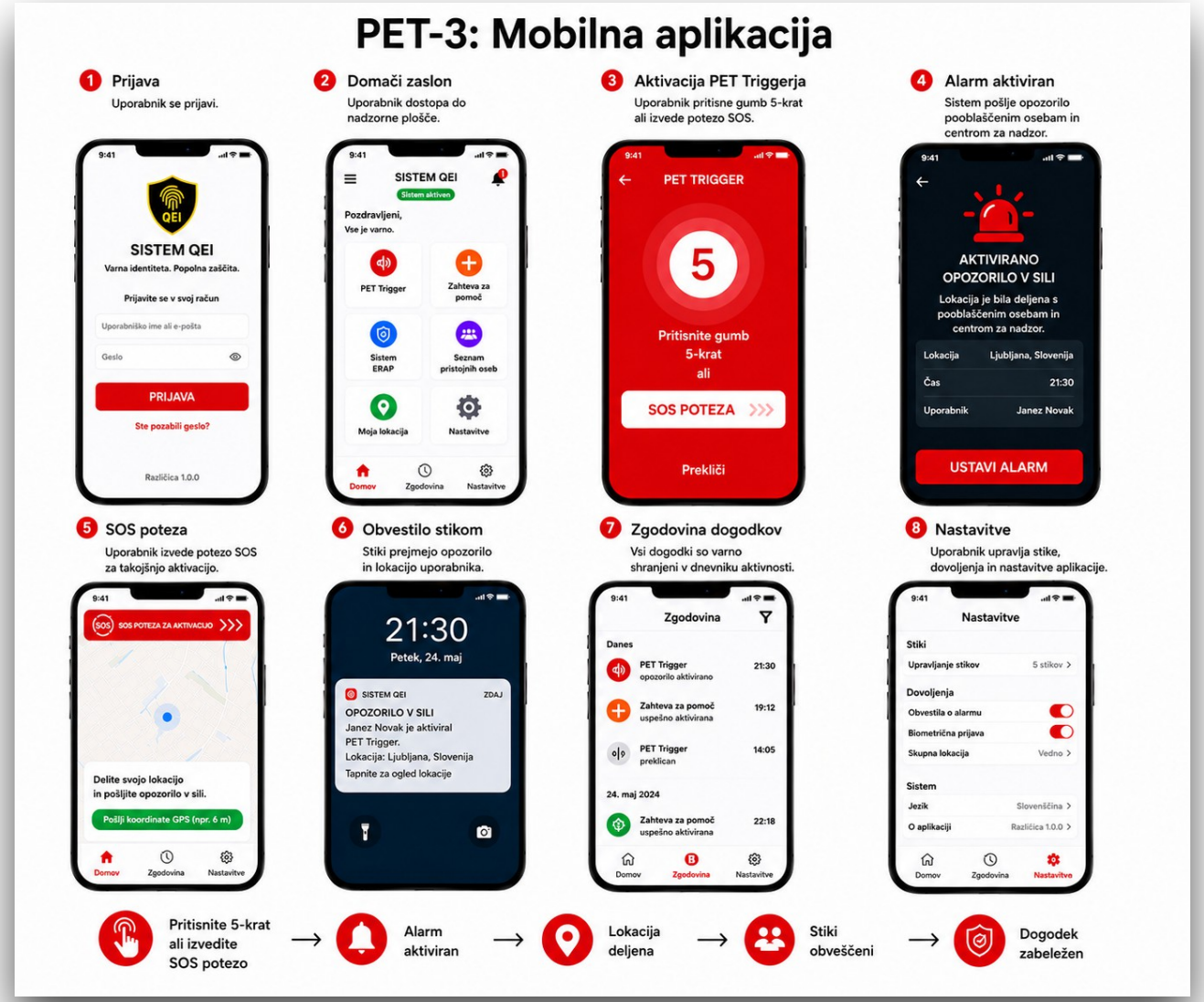
- pubblico,
- autorità competenti.

7.5.4 PET-3: Panic Trigger (dispositivo)

Forma:

- funzione integrata nel telefono cellulare oppure nel dispositivo QEI.





Attivazione:

- combinazione nascosta (ad esempio, pressione del pulsante per cinque volte),
- oppure gesto SOS (*SOS swipe*).

Sicurezza:

- accesso limitato,
- registrazione di tutte le attività (*logging*),
- possibilità di annullamento.

Utilizzo:

- bambino,
- genitore.

7.5.5 Integrazione nel sistema

[Attivatore PET]

↓

[Richiesta di Emergenza (ER)]

↓

[Sistema ERAP]

↓

[Autorità competenti + servizi di monitoraggio delle watchlist]

8. PROPOSTA DI ARCHITETTURA E DEL MODELLO DEI DATI DEL SISTEMA QEI

8.1 Architettura di base

Il sistema proposto si baserebbe su tre livelli separati.

1. Bio Layer

- modelli biometrici,
- modello dell'impronta digitale,
- modello facciale,
- modello biometrico STR trasformato.

2. Crypto Layer

- normalizzazione,
- trasformazione crittografica,
- generazione del token QEI,
- derivazione delle chiavi,
- meccanismo di firma.

3. Access Layer

- autorizzazioni,
- base giuridica,
- audit degli accessi,
- accesso in base ai ruoli degli utenti,
- notifica all'utente.

8.2 Archivi separati

Il sistema dovrebbe basarsi sulla rigorosa separazione di almeno tre archivi.

a) Archivio dell'identità

Archivio esterno separato, che può contenere:

- numero identificativo interno,
- nome e cognome,
- data di nascita,
- cittadinanza,
- stato della persona,
- dati di contatto o del tutore.

Il sistema QEI non dovrebbe conservare tali dati all'interno del token crittografico.

b) Archivio biometrico

Archivio separato contenente modelli biometrici, non dati grezzi:

- *fingerprint template*,
- *facial template*,
- modello STR trasformato limitato,
- data di acquisizione,
- qualità del campione,
- origine del campione,
- stato di validità.

c) Archivio di collegamento QEI

Questo archivio conterrebbe:

- token QEI,
- riferimenti tecnici tra gli archivi,
- registri di audit.

8.3 Principio di funzionamento del sistema

Il funzionamento del sistema seguirebbe la seguente sequenza:

- input biometrico → conversione in modello
- modello → generazione del token QEI o del materiale crittografico
- token o materiale crittografico → confronto oppure procedura di firma
- in caso di corrispondenza → attivazione della procedura autorizzata dalla legge
- solo successivamente → possibile accesso all'archivio esterno dell'identità

8.4 Architettura del sistema definita giuridicamente

Il sistema si basa su tre livelli funzionalmente e giuridicamente separati.

a) Bio Layer

Questo livello contiene esclusivamente modelli biometrici standardizzati e non contiene mai dati biometrici grezzi né dati biologici.

b) Crypto Layer

Questo livello esegue la trasformazione crittografica, la tokenizzazione, la derivazione delle chiavi e le procedure di firma, utilizzando meccanismi crittografici unidirezionali e sicuri.

c) Access Layer

Questo livello contiene le regole di accesso, i meccanismi di audit, la base giuridica per l'accesso ai dati, il controllo giudiziario e i meccanismi decisionali volti a stabilire se la divulgazione dell'identità sia consentita.

Tale architettura garantisce la separazione funzionale, tecnica e giuridica degli elementi essenziali del sistema.

9. TRILOCK - MODELLO DI SICUREZZA A TRE FATTORI

9.1 Struttura di base

La versione più appropriata, sicura e moderna del sistema si basa sulla combinazione di tre fattori biometrici indipendenti che, insieme, costituiscono il modello **TriLock**:

- **K_STR** - materiale crittografico derivato dal modello biometrico STR trasformato,
- **K_FP** - materiale crittografico derivato dall'impronta digitale,
- **K_FACE** - materiale crittografico derivato dalla biometria facciale.

Nessuno di questi elementi lascia il dispositivo in forma grezza o ricostruibile.

9.2 Modello di soglia per l'utilizzo

Il sistema può utilizzare un modello di soglia multilivello:

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

Un tale modello consente di adattare il livello di affidabilità in funzione della sensibilità della singola procedura.

9.3 Combinazione delle chiavi

La chiave finale viene generata combinando più fattori insieme al contesto aggiuntivo del sistema:

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

Si applicano i seguenti principi:

- viene utilizzato **HKDF** o un altro meccanismo sicuro equivalente per la derivazione delle chiavi,
- ogni sistema utilizza il proprio **SALT**,
- ogni finalità d'uso utilizza il proprio **CTX**,
- in questo modo viene garantita la non correlabilità tra i sistemi.

9.4 Principale vantaggio del modello

Il modello **TriLock** consente:

- sicurezza multilivello,
- una significativa riduzione del rischio di falsi positivi,
- una migliore tutela giuridica del sistema,
- una maggiore resistenza agli abusi,
- una più elevata conformità al principio della minimizzazione dei dati.

9.5 Modalità di funzionamento del meccanismo a chiave del QEI

A livello concettuale, il sistema funziona in modo tale che l'utente attiva un fattore biometrico locale, ad esempio l'impronta digitale, dalla quale viene generato un modello biometrico standardizzato.

Questo modello non viene memorizzato né trasmesso nella sua forma grezza, ma viene utilizzato esclusivamente come input locale per la generazione di una firma crittografica monouso.

La procedura si svolge nel modo seguente: il sistema invia una richiesta (*challenge*), mentre il dispositivo, sulla base dei fattori biometrici verificati localmente e del contesto, genera una risposta crittografica univoca.

Il risultato può essere:

- accesso autorizzato,
- accesso negato,
- richiesta di un fattore aggiuntivo.

L'idea fondamentale del sistema è che la biometria non sblocca il sistema come identificatore statico, ma partecipa alla creazione di una chiave digitale monouso o di una firma crittografica.

9.6 QEI ONE - chiave di sicurezza unificata

In alternativa a tre dispositivi separati, è possibile prevedere anche un unico dispositivo fisico:

QEI ONE - chiave di sicurezza unificata

Concetto

QEI ONE riunisce:

- chiave di sicurezza (*Token Access*),
- identificazione (*ID / QR / NFC*),
- *Panic / Emergency Trigger*.

Si tratta di un unico dispositivo fisico che integra più funzioni in un unico supporto di sicurezza.

Come si presenta:



La **QEI ONE** può essere progettata nelle seguenti caratteristiche:

- forma a goccia (*teardrop-shaped form factor*),
- lunghezza di circa **9 cm**,
- larghezza di circa **6 cm**,
- design sottile ed ergonomico (*slim-profile design*).

Strati funzionali

Secure Core

- **Secure Element** (chip di sicurezza),
- conserva i frammenti del sistema **QEI** e il materiale crittografico.

NFC + QEI ID

- funzionalità di identificazione,
- possibilità di attivare una procedura di emergenza tramite scansione (*Emergency Scan*).

Pulsante SOS

- grande pulsante fisico per l'attivazione della procedura di emergenza,
- attiva immediatamente il protocollo **ERAP**.

Indicatore LED

- **verde** = il sistema funziona correttamente,
- **rosso** = modalità di emergenza attivata (*Emergency Mode*),
- **blu** = il dispositivo è attivo oppure connesso.

Batteria

- batteria compatta integrata,
- lunga autonomia di funzionamento.

Come funziona

Utilizzo normale

- il dispositivo viene avvicinato al lettore,
- l'NFC consente l’accesso.

Caso di emergenza

- viene premuto il pulsante SOS,
- oppure viene utilizzata l'impronta digitale,
- il sistema attiva il protocollo **ERAP**.

Architettura in un unico dispositivo

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

Vantaggi

- un unico dispositivo,
- utilizzo più semplice,
- sempre con l'utente,
- maggiore sicurezza,

- più modalità di attivazione,
- non dipende esclusivamente dalla biometria,
- concetto brevettuale più solido di **token hardware multifunzione per l'identità** (*multi-function hardware identity token*).

10. MODELLO BIOMETRICO STR COME FATTORE AGGIUNTIVO

10.1 Ruolo corretto della componente STR

Nel sistema il DNA non viene utilizzato come identificatore permanente, bensì esclusivamente come modello biometrico STR trasformato, dal quale viene generato il materiale crittografico.

Ciò significa che il sistema non si basa sulla conservazione del DNA, ma su una trasformazione tecnica temporanea di un insieme limitato di marcatori identificativi.

10.2 Processo di elaborazione

Il processo può seguire il seguente modello:

STR → vettore numerico → aggiunta del SALT → trasformazione → fuzzy extractor → K_STR

oppure, in modo più dettagliato:

STR → normalizzazione → rappresentazione binaria → aggiunta di SALT + CTX → trasformazione randomizzata → fuzzy extractor → generazione del materiale crittografico K_STR

10.3 Principi fondamentali

- i dati grezzi del DNA vengono eliminati immediatamente dopo l'elaborazione,
- non viene conservato l'intero patrimonio genetico,
- **K_STR** non rappresenta l'identità della persona,
- **K_STR** viene utilizzato esclusivamente come materiale crittografico locale,
- la componente **STR** viene utilizzata unicamente come fattore aggiuntivo per un elevato livello di affidabilità.

10.4 Vantaggio giuridico di questa impostazione

In questo modo il sistema si allontana dal modello del **«DNA come dato»** e si avvicina al modello del **«fattore biometrico trasformato per uso crittografico locale»**, che risulta significativamente più solido sotto il profilo di:

- tutela della privacy,
- principio della minimizzazione dei dati,
- principio della *privacy by design*,
- limitazione della finalità d'uso.

11. AUTENTICAZIONE CRITTOGRAFICA

11.1 Principio challenge-response

Il sistema dovrebbe utilizzare un meccanismo crittografico di tipo **challenge-response**.

La procedura si svolge nel seguente modo:

1. Il server invia una richiesta crittograficamente sicura (*challenge*).
2. Il dispositivo genera localmente oppure sblocca la chiave **K_FINAL**.
3. Il dispositivo firma la richiesta utilizzando la chiave **K_FINAL**.
4. Il server verifica la firma mediante la corrispondente chiave pubblica.

11.2 Cosa il sistema non trasmette mai

Il sistema non trasmette mai:

- dati biometrici grezzi,
- modelli biometrici,
- modello STR,
- il token come identità.

La biometria e i token non vengono utilizzati come mezzo diretto di autenticazione, ma come meccanismo locale di attivazione per la generazione di una firma crittografica.

11.3 Principio *fail-safe*

In caso di dubbio, errore, corrispondenza incompleta o incertezza tecnica, il sistema non rivela l'identità della persona.

Per impostazione predefinita, il sistema deve orientarsi verso il rifiuto dell'accesso oppure verso la richiesta di una verifica aggiuntiva, e non verso la divulgazione dei dati identificativi.

12. ELABORAZIONE LOCALE E MODULI SICURI

12.1 Elaborazione locale

Il sistema deve garantire che tutti i dati biometrici siano elaborati esclusivamente in un ambiente hardware-software sicuro, quale:

- **Trusted Execution Environment (TEE)**,
- **Secure Enclave**,
- oppure un altro modulo di sicurezza equivalente.

12.2 Divieto di esportazione della biometria

I dati biometrici in ingresso:

- non devono lasciare il dispositivo nella loro forma grezza,
- non devono lasciare il dispositivo in una forma ricostruibile,
- non devono essere utilizzati come identificatore globale,
- non devono essere trasferiti a banche dati centrali.

12.3 Conservazione locale delle chiavi

Il dispositivo deve generare e conservare la chiave crittografica privata all'interno del modulo di sicurezza.

I sistemi server non devono conservare dati biometrici né loro rappresentazioni dirette.

12.4 Nessuna banca dati biometrica centrale

Il sistema non crea una banca dati centralizzata di dati biometrici o genetici.

Viene conservato esclusivamente un token crittografico anonimizzato oppure un risultato tecnico minimo che, di per sé, non consente l'identificazione della persona né la ricostruzione della biometria.

13. NOTIFICA ALL'UTENTE E CONTROLLO DELL'UTILIZZO

13.1 Principio di trasparenza dell'utilizzo

Ogni utilizzo del sistema deve essere registrato ai fini dell'audit.

Il registro di utilizzo deve contenere almeno:

- l'ora,
- il servizio o la procedura,
- la posizione oppure l'origine del sistema,
- il risultato dell’utilizzo.

13.2 Notifica all'utente

Quando ciò è giuridicamente e operativamente consentito, l'utente deve ricevere una notifica relativa all'utilizzo del proprio meccanismo di identificazione.

Qualora l'utilizzo non sia stato autorizzato dalla persona legittimata, il sistema deve consentire:

- il blocco di ulteriori utilizzi,
- il ripristino del sistema oppure la sostituzione del materiale crittografico,
- la revoca della chiave esistente,
- l'avvio di una procedura di audit o di sicurezza.

13.3 Audit e responsabilità

Il sistema deve garantire la completa tracciabilità di tutti gli accessi e di tutte le attivazioni delle procedure.

Il registro di audit deve contenere almeno:

- chi ha effettuato l'accesso,
- quando è stato effettuato l'accesso,
- sulla base di quale fondamento giuridico,
- per quale finalità,
- quale è stato il risultato della procedura.

Sul sistema deve essere previsto un meccanismo di controllo indipendente che consenta una valutazione periodica della legalità, della proporzionalità e della sicurezza del suo utilizzo.

14. REVOCA E GESTIONE DEL CICLO DI VITA DELL'IDENTITÀ

14.1 Revoca (*Revocation*)

In caso di compromissione, il sistema deve consentire la sostituzione del materiale identificativo senza modificare le caratteristiche biologiche della persona.

Procedura:

- viene generato un nuovo **SALT**,
- viene eseguita una nuova trasformazione del materiale biometrico,
- viene generata una nuova chiave crittografica,
- la chiave precedente viene disattivata.

14.2 Vantaggio

Ciò significa che il sistema non è statico e consente il ripristino della sicurezza anche dopo un incidente, rappresentando uno dei principali vantaggi rispetto alle tradizionali banche dati biometriche centralizzate.

14.3 Gestione dell'identità senza modificare le caratteristiche biologiche

Il sistema consente di rigenerare il materiale identificativo o crittografico senza la necessità di modificare le caratteristiche biologiche della persona.

Ciò viene ottenuto mediante:

- generazione di un nuovo **SALT**,
- utilizzo di un nuovo contesto (**CTX**), quando necessario,
- nuova trasformazione crittografica,
- generazione di una nuova chiave,
- disattivazione della chiave precedente.

Tale meccanismo riduce in modo significativo il rischio di una compromissione permanente.

15. REQUISITI NORMATIVI

Il sistema dovrebbe soddisfare almeno i seguenti requisiti:

- la biometria è elaborata esclusivamente in locale,
- la componente STR è utilizzata unicamente come modello biometrico trasformato e non riproducibile,
- i token non rappresentano l'identità e non vengono utilizzati per l'autenticazione diretta,
- l'autenticazione si basa sulla firma crittografica,
- il **SALT** deve essere univoco per ogni utente e per ogni sistema,
- il **CTX** deve essere collegato alla finalità d'uso,
- il sistema deve consentire la **revocation**,
- non è consentita una banca dati biometrica centralizzata,
- i sistemi non devono essere crittograficamente collegabili tra loro,
- ogni intervento deve essere tracciabile e giuridicamente limitato.

15.1 Requisiti normativi aggiuntivi

Il sistema deve inoltre garantire:

- la non correlabilità dei token tra sistemi diversi,
- l'utilizzo del **SALT** a livello dell'utente,
- l'utilizzo del **CTX** a livello della finalità,
- una logica di utilizzo multifattoriale,
- il divieto di utilizzare il token come identità diretta,
- il principio della risposta minima del sistema,
- il principio **fail-safe** in caso di risultato incerto,
- la registrazione obbligatoria di audit per tutti gli accessi ai dati.

16. GARANZIE DI SICUREZZA E GIURIDICHE

Il sistema dovrebbe comprendere:

- conservazione separata e cifrata dei dati,
- crittografia multilivello,
- accesso esclusivamente sulla base di una procedura giuridicamente ammissibile,
- organismo di controllo indipendente,
- relazione pubblica annuale,
- test periodici di penetrazione della sicurezza,
- certificazione secondo gli standard di sicurezza delle informazioni,
- meccanismi di sicurezza decentralizzati,
- resilienza a lungo termine delle soluzioni crittografiche.

Qualsiasi abuso o estensione della finalità d'uso dovrebbe essere sanzionabile.

17. QUADRO FINANZIARIO E DI SVILUPPO

17.1 Possibili fonti di finanziamento

- bilancio dello Stato,
- programmi dell'Unione europea,
- progetti di ricerca e sviluppo,
- partenariati pubblico-privati, se giuridicamente ed eticamente ammissibili.

17.2 Stima indicativa dei costi

Ai fini della valutazione preliminare della fattibilità, può essere definita la seguente stima finanziaria indicativa:

- sviluppo del sistema: **2–5 milioni di EUR**,
- progetto pilota: **circa 500.000 EUR**,
- manutenzione annuale: dipendente dall'entità dell'implementazione.

Le possibili fonti di finanziamento comprendono:

- programmi europei (ad esempio **Horizon Europe**, **Digital Europe**, **LIFE**),
- fondi nazionali,
- modelli di finanziamento combinati.

In tale contesto è possibile prevedere un elevato livello di cofinanziamento da parte dell'Unione europea (fino al **90%**), in particolare nell'ambito dei progetti relativi all'identità digitale e alla protezione dei gruppi vulnerabili.

17.3 Proprietà intellettuale e tutela brevettuale

Il sistema proposto **QEI (Quantized Encrypted Identity)** comprende numerose soluzioni originali di natura tecnica, di sicurezza e organizzativa nei settori dell'identità biometrica, della crittografia, della tutela della privacy, della tokenizzazione dell'identità e dell'autenticazione digitale sicura.

Il proponente dell'iniziativa ha predisposto o avviato, presso le autorità competenti in materia di proprietà industriale, procedure di tutela della proprietà intellettuale e di protezione brevettuale per specifici elementi tecnici del sistema.

L'oggetto della tutela può comprendere, tra l'altro:

- il sistema di identità biometrica anonimizzato **QEI_TOKEN**,
- i metodi per la generazione di materiale crittografico a partire da più fattori biometrici indipendenti,
- il modello di sicurezza multifattoriale **TriLock** (STR + impronta digitale + biometria facciale),
- il sistema di archivi separati per dati identificativi, modelli biometrici e registri di audit,
- **QEI ONE** – chiave fisica multifunzionale di identificazione e sicurezza,
- **PET-S (Physical Emergency Trigger Suite)** per l'attivazione di procedure di emergenza senza utilizzo della biometria,

- metodi per l'elaborazione locale dei dati biometrici senza archiviazione centralizzata dei dati biometrici,
- metodi per la tokenizzazione irreversibile dell'identità e la verifica crittografica.

La tutela brevettuale non limita il dibattito pubblico, tecnico o legislativo sull'iniziativa. Il suo scopo è proteggere le soluzioni innovative, prevenire l'appropriazione non autorizzata della proprietà intellettuale e consentire l'ulteriore sviluppo del sistema in collaborazione con gli organi dello Stato, le istituzioni di ricerca, le università, il settore economico e le istituzioni dell'Unione europea.

Il proponente esprime la propria disponibilità a collaborare con la **Repubblica di Slovenia**, con le istituzioni dell'**Unione europea** e con le organizzazioni internazionali per l'ulteriore valutazione tecnica, giuridica e scientifica del sistema.

In caso di ulteriore sviluppo e di un'eventuale implementazione del sistema, potrà essere adottato un adeguato modello di licenza, di partenariato pubblico-privato, di collaborazione nella ricerca oppure un altro modello giuridicamente ammissibile di trasferimento tecnologico, che garantisca la tutela dell'interesse pubblico, dei diritti umani e della protezione dei bambini.

Tutte le future attività di sviluppo dovranno essere svolte nel rispetto della legislazione vigente della **Repubblica di Slovenia**, del diritto dell'**Unione europea**, degli standard internazionali di sicurezza delle informazioni e dei principi di protezione dei dati personali e della privacy.

18. PRESENTAZIONE PUBBLICA E INFORMAZIONE AL PUBBLICO

In caso di ulteriore esame dell'iniziativa, dovrebbe essere garantita una presentazione pubblica trasparente del sistema.

La presentazione pubblica dovrebbe prevedere la partecipazione di:

- costituzionalisti,
- esperti in protezione dei dati personali,
- bioeticisti,
- rappresentanti della società civile,
- esperti nella protezione dei bambini,
- informatici ed esperti di crittografia.

Particolare attenzione dovrebbe essere dedicata alla spiegazione di:

- rigorosa limitazione della finalità,
- misure di protezione tecniche e di sicurezza,
- volontarietà dell'adesione,
- possibilità di cancellazione dei dati,
- controllo giudiziario e indipendente.

Il sistema non deve essere presentato come un meccanismo di sorveglianza generale, bensì esclusivamente come uno specifico strumento di protezione dei bambini.

19. PROPOSTA DEI PASSI SUCCESSIVI

Si propone di:

- organizzare un dibattito pubblico a livello nazionale,
- predisporre un'analisi tecnica della conformità costituzionale,
- predisporre una valutazione della conformità al GDPR e al diritto dell'Unione europea,
- predisporre uno studio tecnico di fattibilità,
- coinvolgere esperti nazionali e internazionali,
- valutare la possibilità di un modello pilota, qualora giuridicamente ammissibile,
- proseguire il dibattito sull'eventuale dimensione europea dell'iniziativa.

In caso di un'eventuale implementazione di successo nella **Repubblica di Slovenia**, l'iniziativa potrebbe essere presentata in futuro anche a livello dell'**Unione europea** e successivamente come iniziativa internazionale per la protezione dei bambini.

19.1 Orientamento strategico dei passi successivi

Per il corretto proseguimento dell'esame dell'iniziativa è opportuno sottolineare che l'obiettivo non è l'introduzione immediata del sistema senza una preventiva valutazione, bensì:

- analisi tecnica,
- validazione giuridica,
- studio tecnico di fattibilità,
- modello pilota, se giuridicamente ammissibile.

L'approccio più solido non è **«introduciamo il sistema»**, bensì **«esaminiamo il sistema come meccanismo complementare di protezione per i casi eccezionali»**.

Tale orientamento:

- riduce le resistenze,
- aumenta l'accettabilità giuridica,
- favorisce il sostegno istituzionale,
- apre la possibilità di finanziamenti a livello dell'Unione europea.

Lo scopo principale dell'iniziativa è rafforzare la protezione dei bambini. Le soluzioni tecnologiche rappresentano soltanto uno strumento di supporto per il raggiungimento di tale obiettivo e devono essere sempre subordinate alla tutela dei diritti umani, della privacy e del superiore interesse del minore.

Il messaggio fondamentale dell'iniziativa è il seguente:

Se esiste una tecnologia che può salvare la vita di un bambino scomparso, è dovere dello Stato verificarne almeno la fattibilità costituzionale, giuridica e tecnica.

19.2 Proposta di progetto pilota

Per passare dal livello concettuale alla verifica operativa, si propone la realizzazione di un progetto pilota.

Possibile quadro del progetto pilota:

- dimensione: **100–500 bambini**,
- durata: **12 mesi**.

Coinvolgimento:

- un ospedale,
- un'unità di polizia,
- un numero limitato di famiglie volontarie.

Obiettivi del progetto pilota:

- verificare la fattibilità tecnica,
- verificare la conformità giuridica nella pratica,
- valutare l'esperienza degli utenti,
- verificare i meccanismi di sicurezza,
- individuare eventuali rischi.

Il progetto pilota rappresenterebbe un passaggio fondamentale prima di un'eventuale implementazione su più ampia scala.

20. PROPOSTA UFFICIALE AL GOVERNO DELLA REPUBBLICA DI SLOVENIA

Proponiamo che il **Governo della Repubblica di Slovenia** esamini la possibilità di avviare un dibattito tecnico e pubblico sull'istituzione di un sistema di identificazione speciale, rigorosamente limitato e volontario, il cui unico scopo sarebbe la protezione dei bambini da:

- tratta di minori,
- sottrazione di bambini alla nascita,
- schiavitù,
- sfruttamento sessuale,
- adozioni illegali,
- altri atti particolarmente gravi lesivi dei diritti dei bambini.

Qualsiasi eventuale soluzione dovrà essere:

- rigorosamente limitata nella finalità,
- sottoposta a controllo giudiziario e indipendente,
- conforme alla **Costituzione della Repubblica di Slovenia**,
- conforme alla legislazione europea,
- progettata tecnicamente in modo da prevenire gli abusi.

21. ARGOMENTI GIURIDICI PER L'ULTERIORE DIBATTITO TECNICO

21.1 Argomenti giuridici approfonditi

Argomenti A FAVORE

- tutela dei bambini come valore costituzionalmente protetto,
- identificazione più rapida dei bambini scomparsi,
- rafforzamento della certezza del diritto nelle procedure particolarmente delicate,
- prevenzione della criminalità organizzata,
- maggiore possibilità di verifica dell'identità nei casi eccezionali.

Argomenti CONTRARI

- interferenza con il diritto alla privacy,
- particolare sensibilità dei dati biometrici e genetici,
- questione della proporzionalità,
- rischio di violazioni della sicurezza o di abusi,
- pericolo di una successiva estensione della finalità d'uso.

Proprio per questo motivo, ogni ulteriore dibattito deve essere rigorosamente fondato sul piano giuridico, tecnicamente verificabile e completamente trasparente.

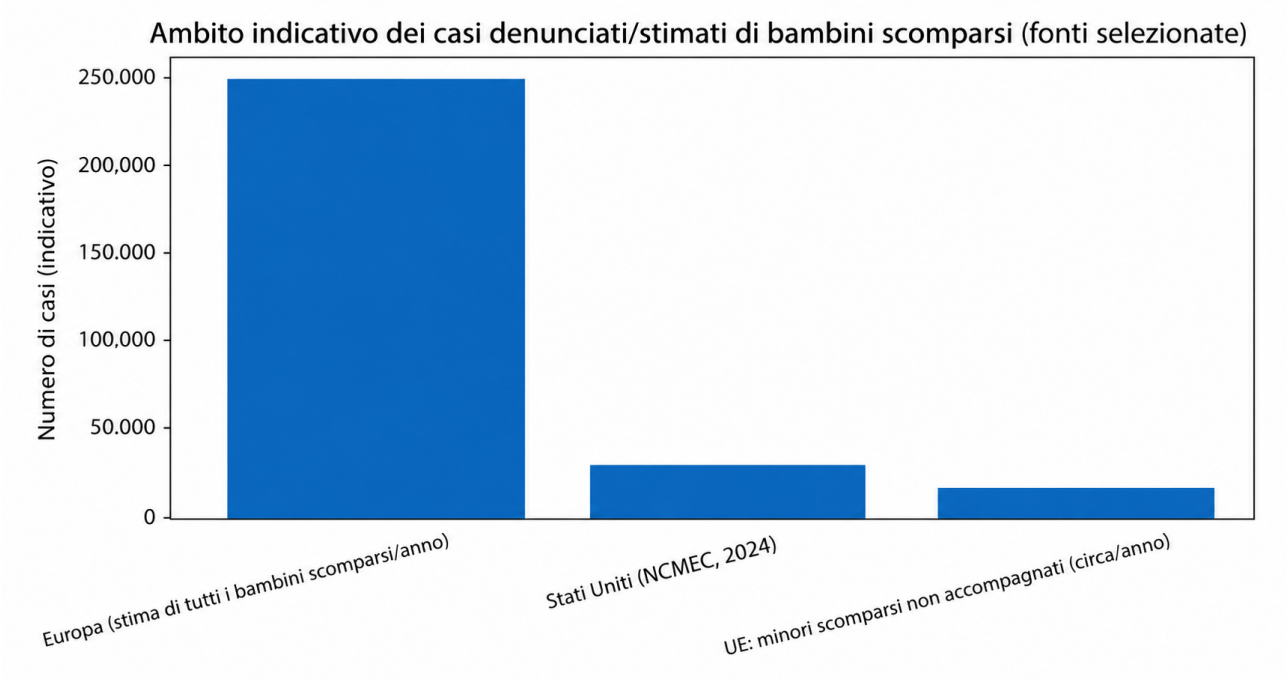
22. PANORAMICA STATISTICA INDICATIVA E ALLEGATI

Questo capitolo presenta una panoramica dei dati internazionali di pubblico dominio che illustrano l'entità del fenomeno dei bambini scomparsi, dei rapimenti di minori e della tratta di esseri umani. A causa delle differenti definizioni giuridiche, delle metodologie di raccolta dei dati e dei registri nazionali, un confronto diretto tra i singoli Paesi non è sempre possibile. Lo scopo dei dati presentati è quello di fornire un quadro indicativo dell'entità del fenomeno e di sostenere il dibattito tecnico sulla necessità di ulteriori meccanismi di protezione dei bambini.

22.1 Panoramica statistica indicativa

Per una migliore comprensione della portata del fenomeno oggetto della presente iniziativa, di seguito sono presentati alcuni indicatori statistici selezionati provenienti dagli **Stati Uniti d'America**, dall'**Europa** e dal contesto mondiale.

La panoramica si basa sui dati del **National Center for Missing & Exploited Children (NCMEC)**, del **National Crime Information Center (NCIC)**, dell'organizzazione **Missing Children Europe**, dell'**Unione europea** e dell'**United Nations Office on Drugs and Crime (UNODC)**.



I dati presentati dimostrano che il problema dei bambini scomparsi, dei rapimenti e della tratta di esseri umani rappresenta una sfida globale. Sebbene le metodologie di raccolta dati varino da paese a paese, tutte le fonti disponibili confermano la necessità di sviluppare ulteriormente meccanismi di protezione efficaci per i minori.

Regione	**Minori scomparsišani / izginuli otroci**	**Rapimenti / sequestri**	**Tratta di esseri umani / minori**
Stati Uniti	• NCMEC (2024): 29.568 segnalazioni di minori scomparsi. • NCIC (2024): 349.557 segnalazioni di persone scomparse.	• 2.366 rapimenti da parte di un genitore privo dell'affidamento. • 293 rapimenti da parte di persone sconosciute.	• Circa 1 caso su 7 di fuga ad alto rischio è associato al rischio di tratta di esseri umani.
Europa	• Circa 250.000 segnalazioni di minori scomparsi ogni anno. • 2021–2023: almeno 51.433 minori migranti scomparsi.	• Non esiste una statistica unica dell'UE; i dati sono frammentati tra i vari Paesi.	• L'UNODC segnala diverse forme di sfruttamento dei minori; le percentuali variano da Paese a Paese.
Globale	• Non esiste una statistica mondiale comparabile unificata.	• Non esiste una statistica globale unificata sui rapimenti di minori.	• UNODC (2022): 69.627 vittime accertate della tratta di esseri umani; i minori rappresentano circa il 38% delle vittime accertate.

Nota: I dati sono indicativi e destinati a una rappresentazione comparativa. A causa delle differenze nelle definizioni giuridiche e nelle metodologie adottate, il confronto diretto tra i diversi Paesi non è sempre possibile.

Fonti: NCMEC, NCIC, Missing Children Europe, Unione europea, UNODC – *Global Report on Trafficking in Persons*.

22.2 Rapimenti o sottrazioni di neonati dagli ospedali

I rapimenti o le sottrazioni di neonati dagli ospedali rappresentano una delle forme più delicate di reati contro i bambini. Tali casi sono statisticamente rari nella maggior parte dei Paesi sviluppati, ma, a causa delle conseguenze permanenti per il bambino, i genitori e la società, rivestono un'importanza eccezionalmente elevata.

A causa della mancanza di uniformità nelle definizioni giuridiche, delle diverse modalità di segnalazione e della frammentazione dei registri, attualmente non esiste una statistica mondiale unificata che consenta un confronto diretto tra i diversi Paesi. I singoli Stati mantengono registri basati su criteri differenti, per cui i confronti internazionali risultano limitati.

Nonostante la loro rarità, tali casi rappresentano una delle più gravi violazioni dei diritti del bambino. Per questo motivo, numerosi esperti sottolineano l'importanza delle misure preventive, della rapida identificazione dei bambini e di un'efficace cooperazione tra le strutture sanitarie, la polizia, le autorità giudiziarie e i servizi sociali.

Il sistema **QEI** proposto è concepito come un meccanismo di protezione volontario, rigorosamente limitato dalla legge e rispettoso della privacy, il cui scopo non è il controllo delle persone, bensì fornire un supporto per una più rapida identificazione dei bambini nei casi eccezionali di rapimento, sottrazione illegale o tratta di esseri umani.

Sebbene tali casi siano statisticamente rari, le loro conseguenze per il bambino, la famiglia e la società giustificano una riflessione su ulteriori meccanismi di protezione che, nel rispetto dei diritti umani, della privacy e del principio della volontarietà, possano consentire una più rapida identificazione del bambino in circostanze eccezionali.

22.3 Tratta di esseri umani a livello globale - quota dei bambini

La tratta di esseri umani rimane una delle più gravi forme di criminalità organizzata e una delle più serie violazioni dei diritti umani. I bambini rappresentano un gruppo particolarmente vulnerabile, poiché sono spesso vittime di sfruttamento sessuale, lavoro forzato, accattonaggio forzato, adozioni illegali e di altre forme di sfruttamento.

Secondo i dati delle **Nazioni Unite (UNODC)**, nel **2022** sono state registrate a livello mondiale **69.627 vittime accertate di tratta di esseri umani**, delle quali i bambini rappresentavano circa il **38%** del totale delle vittime individuate.

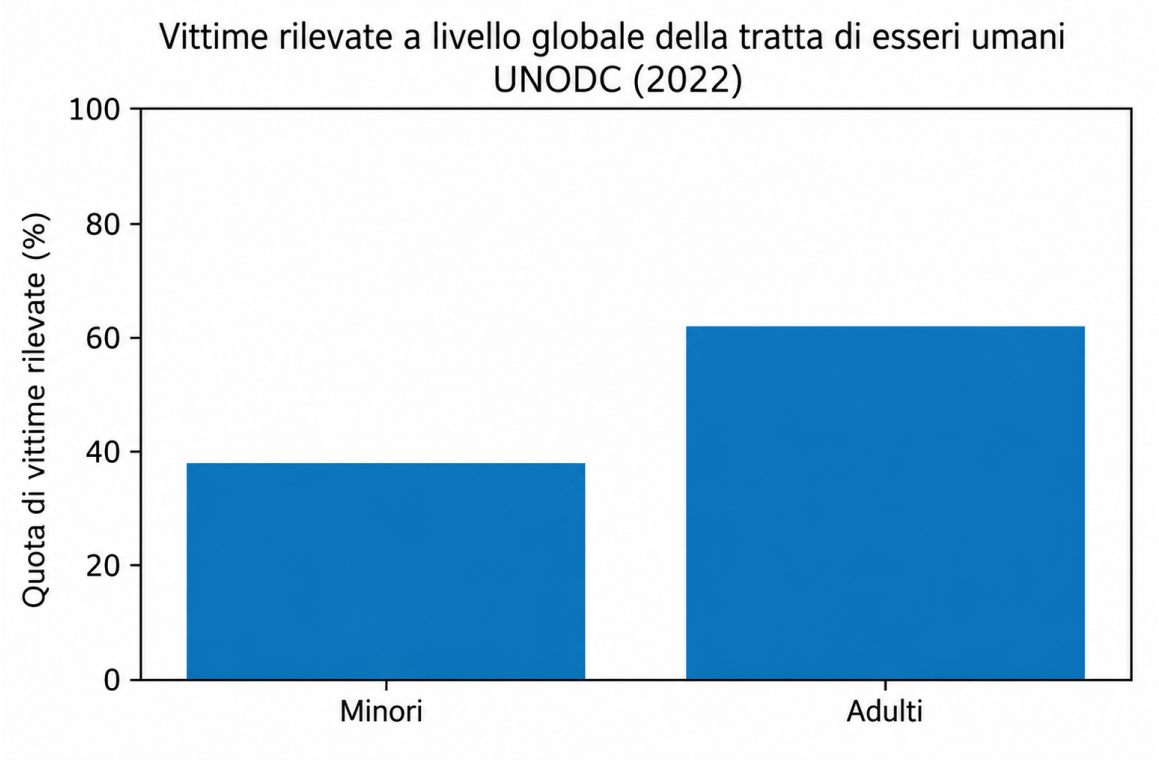


Figura: Proporzione di bambini e adulti tra le vittime di tratta di esseri umani individuate (UNODC, 2022).

Indicatore	Valore
Vittime registrate di tratta di esseri umani (UNODC, 2022)	**69.627**
Proporzione di bambini tra le vittime individuate	**38 %**
Percentuale di adulti tra le vittime individuate	**62 %**

Fonte: *Ufficio delle Nazioni Unite contro la droga e il crimine (UNODC), Rapporto globale sulla tratta di persone 2024.*

22.4 Fonti per il materiale di accompagnamento / Note

I dati riportati nel capitolo 22 si basano su relazioni pubblicamente disponibili, statistiche ufficiali e pubblicazioni di organizzazioni internazionali. A causa delle diverse definizioni giuridiche, delle metodologie di raccolta dei dati e dei sistemi nazionali di registrazione, il confronto diretto tra i singoli Paesi non è sempre possibile. Lo scopo delle fonti riportate è fornire una base tecnica per il dibattito sulla protezione dei bambini e illustrare la portata del fenomeno in esame.

Fonti utilizzate:

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. Unione europea

- European Parliament Research Service (EPRS)
- *Disappearance of Migrant Children in the European Union*
- Commissione europea
- 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

Nota metodologica

I dati numerici utilizzati nel presente documento rappresentano una panoramica indicativa delle informazioni pubblicamente disponibili e non costituiscono una statistica internazionale unificata. Le differenze tra i vari Paesi derivano da differenti definizioni giuridiche, registri nazionali, metodologie di raccolta dei dati e modalità di rendicontazione da parte delle autorità competenti. Di conseguenza, il confronto diretto tra i singoli Paesi non è sempre metodologicamente appropriato.

Lo scopo dei dati presentati non è quello di elaborare un'analisi statistica completa, bensì di illustrare la portata del fenomeno dei bambini scomparsi, dei rapimenti di minori e della tratta di esseri umani quale base tecnica per il dibattito sull'introduzione di ulteriori meccanismi di protezione.

23. CONCLUSIONE

La presente costituisce un'iniziativa volta a promuovere una riflessione, una valutazione tecnica e un dibattito pubblico su una possibile disciplina legislativa in un ambito particolarmente delicato quale la protezione dei bambini.

L'obiettivo dell'iniziativa non è l'istituzione di un sistema generale di sorveglianza, bensì l'esame della possibilità di sviluppare un meccanismo di protezione rigorosamente limitato, conforme alla Costituzione, tecnicamente sicuro e giuridicamente controllato, destinato esclusivamente alla protezione dei bambini nei casi più gravi e delicati.

Il modello tecnico proposto si basa sulla combinazione di tre fattori biometrici indipendenti in un'unica chiave crittografica, che esiste esclusivamente sul dispositivo dell'utente e che non può essere facilmente rubata, copiata o utilizzata al di fuori del sistema rigorosamente definito.

Qualsiasi ulteriore valutazione di un sistema di questo tipo deve basarsi su:

- volontarietà,
- minimizzazione dei dati,
- tokenizzazione irreversibile,
- separazione degli archivi,
- controllo giudiziario,
- audit indipendente,
- pieno rispetto dei diritti umani.

È inoltre importante sottolineare che il sistema proposto non è destinato a collegare gli archivi pubblici esistenti né a creare una banca dati centralizzata di dati biometrici o genetici. Il sistema è concepito come un meccanismo decentralizzato, gestito dall'utente, che consente la verifica dell'identità esclusivamente nei casi eccezionali in cui i sistemi esistenti non garantiscono un'identificazione affidabile e soltanto sulla base di un'adeguata base giuridica.

L'iniziativa proposta non costituisce pertanto una proposta di immediata introduzione di un nuovo sistema, bensì un invito a un dibattito responsabile, tecnico e trasparente sulle possibilità di sviluppare un ulteriore meccanismo di protezione che, nel rigoroso rispetto dei diritti umani, della tutela della privacy e dell'ordinamento giuridico vigente, possa contribuire a una più efficace protezione dei bambini.

La decisione finale in merito all'eventuale ulteriore elaborazione della normativa o alla realizzazione di un progetto pilota dovrà basarsi su analisi tecniche, valutazioni giuridiche, fattibilità tecnica e un ampio consenso sociale. Solo in questo modo sarà possibile garantire che le eventuali soluzioni future siano al tempo stesso efficaci, proporzionate, conformi alla Costituzione e orientate al superiore interesse del bambino.

24. FONTI E BIBLIOGRAFIA

24.1 Atti giuridici internazionali

- Dichiarazione universale dei diritti umani (Organizzazione delle Nazioni Unite, 1948).
- Convenzione delle Nazioni Unite sui diritti dell'infanzia (1989).
- Convenzione europea dei diritti dell'uomo.
- Carta dei diritti fondamentali dell'Unione europea.

24.2 Legislazione dell'Unione europea

- Regolamento generale sulla protezione dei dati (**GDPR**).
- Regolamento sull'identità digitale europea (**eIDAS**).
- Regolamento dell'Unione europea sull'intelligenza artificiale (**AI Act**).

24.3 Legislazione nazionale della Repubblica di Slovenia

- Costituzione della Repubblica di Slovenia.
- Legge sulla protezione dei dati personali (**ZVOP-2**).
- Codice penale (**KZ-1**).
- Codice di procedura penale (**ZKP**).
- Codice della famiglia.
- Legge sui compiti e i poteri della Polizia (**ZNPPol**).

24.4 Standard internazionali e linee guida tecniche

Nella preparazione dell'iniziativa sono stati presi in considerazione anche principi e raccomandazioni generalmente riconosciuti nei seguenti ambiti:

- sicurezza informatica e cybersicurezza,
- protezione dei dati personali,
- tutela dei dati biometrici,
- metodi crittografici,
- identità digitale,
- protezione dei bambini,
- prevenzione della tratta di esseri umani.

Sono stati inoltre presi in considerazione le raccomandazioni e gli standard delle seguenti organizzazioni internazionali:

- Organizzazione Internazionale per la Normazione (**ISO**),
- Agenzia dell'Unione europea per la cybersicurezza (**ENISA**),
- National Institute of Standards and Technology degli Stati Uniti (**NIST**),
- Europol,
- Interpol,
- UNICEF,
- Organizzazione per la Cooperazione e lo Sviluppo Economico (**OCSE / OECD**),
- Organizzazione delle Nazioni Unite (**ONU / UN**).

24.5 Letteratura tecnica

Nella preparazione dell'iniziativa sono state prese in considerazione anche opere tecniche generalmente riconosciute nei settori di:

- crittografia,
- sicurezza delle informazioni,
- identità digitale,
- tutela della privacy,
- sistemi biometrici,
- protezione dei bambini e diritti umani.

Nota

La presente iniziativa si basa sulla legislazione vigente della **Repubblica di Slovenia**, sul diritto dell'**Unione europea**, sulle convenzioni internazionali e sui principi tecnici generalmente riconosciuti nei settori della tutela dei diritti umani, della protezione dei bambini, dell'identità digitale, della sicurezza delle informazioni e della protezione dei dati personali.

25. GLOSSARIO DEI TERMINI CHIAVE, DELLE ABBREVIAZIONI E DEI TERMINI STRANIERI

Per facilitare la comprensione dell'iniziativa, di seguito sono spiegati i principali termini tecnici, le abbreviazioni e i termini stranieri utilizzati nel presente documento.

QEI (Quantized Encrypted Identity)
Sistema di identificazione protetto crittograficamente che genera, a partire da modelli biometrici standardizzati, un token di identificazione anonimizzato per la verifica dell'identità nell'ambito di procedure rigorosamente limitate.

Token
Registrazione crittografica o tecnica di identificazione che, di per sé, non contiene l'identità diretta della persona.

Biometria
Utilizzo delle caratteristiche fisiche o comportamentali uniche di una persona (ad esempio impronta digitale, volto, iride o voce) per verificare o confermare l'identità.

Modello biometrico
Rappresentazione tecnica standardizzata di determinate caratteristiche biometriche, diversa dal dato biometrico grezzo.

Token di identificazione biometrica
Identificatore crittografico anonimizzato generato da modelli biometrici standardizzati, che non contiene dati personali e non consente la ricostruzione della biometria né l'identificazione diretta della persona.

STR (Short Tandem Repeat)
Breve sequenza ripetuta di DNA che può essere utilizzata, in forma trasformata, come fattore biometrico aggiuntivo.

Crittografia
Disciplina che studia i metodi di protezione dei dati mediante algoritmi matematici, garantendo riservatezza, integrità e autenticità delle informazioni.

Chiave crittografica
Valore digitale utilizzato per la cifratura, l'autenticazione o la derivazione di altre chiavi di sicurezza.

Tokenizzazione crittografica
Processo di trasformazione dei dati biometrici o di altri dati di ingresso in una rappresentazione crittografica irreversibile che consente di verificare la corrispondenza senza rivelare i dati originali.

Funzione hash (funzione crittografica di hashing)
Funzione matematica che trasforma i dati di ingresso in una rappresentazione univoca e irreversibile di lunghezza fissa.

Trasformazione irreversibile
Procedura crittografica che non consente di ricostruire i dati originali a partire dal risultato generato.

Autenticazione
Procedura di verifica che una persona, un dispositivo o un sistema sia effettivamente ciò che dichiara di essere.

Autenticazione multifattoriale
Metodo di verifica dell'identità che utilizza due o più fattori di sicurezza indipendenti per autorizzare l'accesso.

Autorizzazione
Procedura che determina a quali dati o funzioni un utente può accedere dopo un'autenticazione riuscita.

Traccia di audit
Registrazione elettronica di tutti gli accessi, delle verifiche e dell'utilizzo del sistema, che consente il controllo successivo della legittimità e della tracciabilità delle procedure.

Archivi separati
Principio secondo il quale i dati identificativi, i modelli biometrici e i registri di audit sono conservati in archivi distinti, riducendo significativamente il rischio di abusi e di accessi non autorizzati.

Architettura decentralizzata
Architettura di un sistema informativo nella quale i dati sensibili non sono conservati in un'unica banca dati centrale, ma sono separati e protetti in diversi livelli di sicurezza o archivi.

Identità decentralizzata (DID – Decentralized Identity)
Modello di identità digitale nel quale l'utente mantiene il controllo della propria identità senza un gestore centrale.

Verifiable Credentials (VC)
Credenziali digitali la cui autenticità può essere verificata crittograficamente.

Root of Trust
Fondamento di fiducia del sistema; quadro giuridico o tecnico che garantisce l'affidabilità e la sicurezza del funzionamento del sistema.

Challenge–Response (sfida-risposta crittografica)
Meccanismo di sicurezza nel quale il sistema invia una sfida crittografica e il dispositivo restituisce una risposta crittografica verificabile.

Threat Model (modello delle minacce)
Analisi strutturata delle possibili minacce, attacchi e abusi del sistema.

Deepfake
Contenuto digitale creato o modificato mediante intelligenza artificiale che può rappresentare falsamente il volto, la voce o l'identità di una persona.

Privacy by Design
Principio secondo il quale la tutela della privacy è integrata fin dalla progettazione del sistema.

Privacy by Default
Principio secondo il quale le impostazioni predefinite del sistema garantiscono fin dall'inizio il massimo livello possibile di tutela della privacy.

Pseudonimizzazione
Procedura mediante la quale i dati personali vengono sostituiti con un identificatore, rendendo impossibile identificare direttamente la persona senza informazioni aggiuntive.

Anonimizzazione
Procedura di eliminazione permanente della possibilità di identificare una persona, rendendo impossibile risalire alla sua identità.

Secure Enclave
Modulo di elaborazione isolato e sicuro destinato all'elaborazione locale di dati sensibili e alla conservazione sicura delle chiavi crittografiche.

Trusted Execution Environment (TEE)
Ambiente di esecuzione affidabile che consente l'esecuzione protetta di operazioni sensibili alla sicurezza, separatamente dal resto del sistema.

Secure Element
Chip di sicurezza dedicato alla conservazione protetta delle chiavi crittografiche e all'esecuzione di operazioni di sicurezza sensibili.

Revocation (revoca)
Procedura di revoca o invalidazione di un elemento identificativo o crittografico.

Recovery (ripristino del sistema)
Procedura di ripristino dell'accesso o del sistema dopo perdita, furto o compromissione.

HKDF (HMAC-based Key Derivation Function)
Metodo crittografico per la derivazione sicura di nuove chiavi a partire da materiale crittografico esistente.

SALT
Valore casuale aggiunto ai dati prima dell'elaborazione crittografica, che aumenta la sicurezza e impedisce risultati prevedibili.

CTX (Context)
Contesto d'uso associato a una specifica finalità o ambiente, che impedisce la correlazione dei risultati tra sistemi diversi.

Progetto pilota
Sperimentazione limitata del sistema nella pratica, finalizzata a verificarne la fattibilità tecnica, giuridica e operativa.

ERAP (Emergency Response Activation Protocol)
Protocollo per l'attivazione delle procedure in situazioni di emergenza.

Emergency Request (ER)
Richiesta crittograficamente protetta per l'attivazione di una procedura di emergenza nell'ambito del sistema QEI.

PET-S (Physical Emergency Trigger Suite)
Insieme di attivatori fisici per situazioni di emergenza che consentono l'attivazione del sistema senza l'utilizzo della biometria.

Family Token
Elemento di identificazione crittografico destinato a collegare i membri della stessa famiglia all'interno del sistema QEI senza rivelarne l'identità.

TriLock
Modello di sicurezza multifattoriale che combina tre fattori biometrici indipendenti (modello biometrico STR trasformato, impronta digitale e biometria facciale) per generare un'unica chiave crittografica.

QEI ONE
Dispositivo di sicurezza multifunzionale proposto, che integra identificazione, protezione crittografica e funzioni per l'attivazione delle procedure di emergenza.

Logging (registrazione degli eventi)
Registrazione automatica di tutti gli eventi di sicurezza, degli accessi e delle procedure rilevanti, al fine di garantire tracciabilità e controllo.

Zero Trust
Modello di sicurezza nel quale nessun dispositivo o utente è considerato automaticamente affidabile, ma ogni richiesta viene verificata singolarmente.

Fail-safe
Modalità di funzionamento del sistema nella quale, in caso di errore, il sistema passa a uno stato sicuro senza compromettere la sicurezza o la privacy.

Interoperabilità
Capacità di sistemi differenti di collaborare tra loro in modo tecnicamente e giuridicamente compatibile.

Standard di interoperabilità
Standard tecnico condiviso che consente la connettività e la cooperazione tra diversi sistemi informativi.

API (Application Programming Interface)
Interfaccia software standardizzata che consente una comunicazione sicura tra diversi sistemi informativi.

eIDAS 2.0
Quadro giuridico europeo relativo all'identità elettronica, all'identificazione elettronica e ai servizi fiduciari.

GDPR (General Data Protection Regulation)
Regolamento generale dell'Unione europea sulla protezione dei dati personali, che stabilisce le norme per il trattamento lecito dei dati personali.

Principio del minimo privilegio (Least Privilege)
Principio della sicurezza delle informazioni secondo il quale ogni utente o sistema dispone esclusivamente delle autorizzazioni strettamente necessarie per svolgere i propri compiti.

ALLEGATO I - INTEGRAZIONE TECNICA AGGIUNTIVA: ELEMENTI CHIAVE MANCANTI PER UNA REALE IMPLEMENTAZIONE

I.1 Root of Trust

L'attuale livello concettuale prevede un livello di certificazione o di convalida, ma, ai fini della validità giuridica e dell'affidabilità del sistema, deve essere chiaramente definito chi rappresenti effettivamente il **Root of Trust** del sistema.

La questione fondamentale è:

- se il fondamento della fiducia sia lo Stato,
- se si tratti di un quadro europeo di fiducia,
- se sia possibile un soggetto privato, ma rigorosamente regolamentato,
- se il sistema debba essere collegato al quadro **eIDAS**.

Senza un **Root of Trust** chiaramente definito non è possibile garantire:

- la validità giuridica delle firme,
- la fiducia istituzionale,
- il reciproco riconoscimento dei risultati,
- l'utilizzo operativo nelle procedure ufficiali.

Per questo motivo, nella successiva fase tecnica dovrà essere chiaramente stabilito che il fondamento della fiducia dovrà essere collocato all'interno:

- dell'ordinamento giuridico nazionale,
- del quadro europeo dell'identità elettronica,
- oppure di un altro sistema di elevato livello di fiducia previsto dalla legge.

I.2 Base giuridica (GDPR + eIDAS + quadro nazionale)

Non è sufficiente che il sistema non conservi dati grezzi. Il diritto, infatti, non disciplina soltanto la conservazione dei dati, ma anche:

- il trattamento,
- la finalità,
- la base giuridica,
- il titolare del trattamento,
- i diritti dell'interessato,
- le misure di sicurezza,
- le procedure di cancellazione e revoca.

Pertanto, ogni futura versione del progetto dovrebbe definire espressamente:

- la base giuridica ai sensi dell'articolo 6 del GDPR,
- la base giuridica per il trattamento delle categorie particolari di dati ai sensi dell'articolo 9 del GDPR,

- il rapporto con l'interesse pubblico,
- il rapporto con il consenso esplicito,
- il ruolo del titolare e del responsabile del trattamento,
- il diritto alla cancellazione,
- il diritto all'informazione,
- il diritto all'audit degli interventi,
- il rapporto con il futuro quadro **eIDAS 2.0**.

I.3 Gestione delle chiavi (Key Management)

Uno dei principali aspetti ancora aperti del sistema riguarda la gestione delle chiavi e del ciclo di vita del materiale identificativo.

Occorre rispondere almeno alle seguenti domande:

- cosa accade se l'utente perde il token,
- se perde l'accesso alla propria identità,
- come avviene il ripristino,
- come viene eseguita la revoca,
- come si previene l'abuso in caso di furto o compromissione.

Il sistema deve pertanto prevedere obbligatoriamente:

- un meccanismo di ripristino (*Recovery*),
- un meccanismo di revoca (*Revocation*),
- una procedura di ripristino multifattoriale,
- la possibilità di coinvolgere un modello di conferma familiare o istituzionale,
- la disattivazione del token compromesso, tracciabile sotto il profilo temporale e giuridico.

I.4 Standard e interoperabilità

Attualmente il sistema è descritto come un quadro concettuale autonomo. Per un utilizzo reale, tuttavia, deve essere interoperabile con i sistemi esistenti.

È necessario definire almeno:

- il formato del token,
- gli standard di trasmissione,
- i meccanismi API,
- le regole di comunicazione,
- la compatibilità con i sistemi statali,
- la conformità ai quadri europei dell'identità digitale.

Se il sistema non è interoperabile, rimane un concetto chiuso, privo di reale utilità in:

- procedure di polizia,
- casi transfrontalieri,
- ambiente ospedaliero,
- procedure amministrative,
- sistemi europei interoperabili.

I.5 Flusso di verifica (Verification Flow)

Per garantire la credibilità giuridica e tecnica non è sufficiente descrivere il solo token. È necessario definire con precisione anche il processo di verifica dell'identità.

Occorre descrivere:

- chi avvia la procedura,
- chi visualizza i singoli frammenti,
- chi li ricompone,
- chi verifica il risultato crittografico,
- chi può autorizzare l'accesso all'archivio dell'identità,
- a quali condizioni l'identità può essere effettivamente rivelata.

Ciò significa che il documento successivo dovrà contenere un flusso procedurale dettagliato di verifica per ciascuno dei principali scenari d'uso.

I.6 Attacchi e abusi

Qualsiasi seria valutazione istituzionale o europea affronterà tra i primi aspetti il tema delle minacce, degli attacchi e dei possibili abusi.

È necessario definire almeno:

- il furto del token,
- la clonazione del dispositivo,
- gli attacchi mediante tentativi di password o chiavi,
- gli attacchi alle comunicazioni,
- il social engineering,
- la compromissione dell'autorità di certificazione,
- gli attacchi al dispositivo dell'utente,
- gli abusi interni al sistema.

Pertanto, il successivo sviluppo dovrà essere integrato con:

- un modello formale delle minacce (*Threat Model*),
- un'architettura di sicurezza,
- meccanismi anti-clonazione,
- un approccio basato su un chip di sicurezza (*Secure Element*),
- registri di audit,
- meccanismi per il blocco d'emergenza e il ripristino del sistema.

I.7 Scenari reali di utilizzo

Per garantirne l'accettabilità operativa è essenziale che il sistema non rimanga un concetto puramente astratto, ma includa chiari scenari di utilizzo reale.

Tali scenari dovrebbero comprendere almeno:

- il caso di un bambino scomparso,
- il caso di sospetta adozione illegale,

- il caso della verifica della parentela nell'ambito di una procedura legalmente consentita,
- il caso di un attivatore fisico per situazioni di emergenza,
- il caso di un'identificazione autorizzata dall'autorità giudiziaria in un caso particolarmente delicato.

Solo scenari concreti consentono di valutare:

- la proporzionalità,
- l'ammissibilità giuridica,
- la fattibilità tecnica,
- l'utilità operativa.

I.8 Finanziamento e governance

Per qualsiasi progetto serio è necessario affrontare fin dall'iniziativa anche le seguenti questioni:

- chi finanzia il sistema,
- chi gestisce l'infrastruttura,
- chi ne assume la responsabilità,
- chi esercita il controllo,
- chi sostiene i costi della certificazione,
- chi garantisce la manutenzione a lungo termine.

Senza una risposta a queste domande, nessun sistema può passare dal livello di semplice idea a quello di una reale valutazione istituzionale.

ALLEGATO II - INTEGRAZIONE AGGIUNTIVA SULLA SICUREZZA: THREAT MODEL, ARCHITETTURA DI SICUREZZA E ORIENTAMENTO ALLA CERTIFICAZIONE

II.1 Premessa fondamentale sulla sicurezza

Ogni sistema può teoricamente essere attaccato. Tuttavia, la differenza essenziale tra i sistemi consiste nella difficoltà dell'attacco, nell'entità dei danni che esso può causare e nella capacità dell'architettura di ridurre fin dall'origine i rischi sistemici.

Il sistema **QEI** può essere significativamente più resiliente rispetto ai tradizionali modelli centralizzati, se correttamente progettato, poiché:

- non dispone di una banca dati centrale contenente dati sensibili,
- utilizza la frammentazione,
- utilizza la trasformazione locale,
- impiega meccanismi crittografici,
- consente la conservazione separata dei diversi livelli del sistema.

II.2 Principali superfici di attacco

Un attaccante può prendere di mira in particolare i seguenti livelli:

- l'utente,
- il token fisico,
- il dispositivo dell'utente,
- la comunicazione,
- il livello di certificazione o istituzionale,
- le procedure di ripristino e revoca,
- il social engineering.

I rischi reali più significativi non risiedono necessariamente nella crittografia matematica, bensì in:

- errore umano,
- furto del dispositivo fisico,
- inganno dell'utente,
- gestione inadeguata delle chiavi,
- abusi interni.

II.3 Attacchi tipici e misure di protezione proposte

a) Furto del token

Lo scenario di attacco più realistico è il furto fisico del dispositivo o del supporto.

Misure di protezione proposte:

- protezione mediante codice PIN,

- ritardo temporale dopo tentativi errati,
- possibilità di disattivazione immediata,
- chip di sicurezza (*Secure Element*),
- funzionalità limitata senza un ulteriore fattore di autenticazione.

b) Social engineering

L'attacco è spesso diretto all'utente e non al sistema.

Misure di protezione proposte:

- conferma a più livelli,
- avvisi chiari all'utente,
- notifiche sull'utilizzo,
- formazione degli utenti,
- blocco di emergenza (*emergency lock*).

c) Attacco al dispositivo

L'attaccante può prendere di mira il telefono, il computer o un altro dispositivo.

Misure di protezione proposte:

- **Trusted Execution Environment (TEE)**,
- **Secure Enclave**,
- isolamento delle chiavi,
- divieto di esportazione del materiale sensibile,
- firma esclusivamente all'interno del modulo di sicurezza.

d) Attacco alla comunicazione

Sono possibili attacchi *man-in-the-middle* o intercettazioni delle richieste.

Misure di protezione proposte:

- crittografia end-to-end,
- richieste firmate digitalmente,
- meccanismo *challenge-response*,
- verifica dell'integrità delle richieste.

e) Attacco alle istituzioni

L'attacco può essere rivolto all'autorità di certificazione o di firma.

Misure di protezione proposte:

- nessuna conservazione di dati biometrici grezzi,
- rigorosa separazione delle funzioni,
- tracciabilità di audit,
- controllo multilivello,
- verifiche periodiche della sicurezza.

II.4 Architettura di sicurezza a livelli

La progettazione raccomandata del sistema deve seguire il principio della **difesa multilivello (*defense-in-depth*)**.

Layer 1 - Device Security

- chip di sicurezza (*Secure Element*),
- protezione contro la manomissione del dispositivo (*anti-tamper*),
- conservazione cifrata dei dati.

Layer 2 - Crypto Layer

- hashing o trasformazione della biometria,
- firme digitali,
- isolamento delle chiavi,
- **HKDF** o procedure equivalenti di derivazione delle chiavi.

Layer 3 - Communication Layer

- crittografia end-to-end,
- richieste firmate digitalmente,
- verifica dell'integrità.

Layer 4 - Policy Layer

- controllo familiare,
- accesso adattabile,
- regole giuridiche di accesso,
- condizioni giudiziarie o istituzionali per l'attivazione.

Layer 5 - Emergency Layer

- **ERAP**,
- blocco di emergenza (*emergency lock*),
- ripristino del sistema (*Recovery*),
- revoca (*Revocation*).

L'idea fondamentale della sicurezza è che un attaccante debba compromettere contemporaneamente più livelli del sistema e non un unico punto di vulnerabilità.

II.5 Orientamento alla certificazione e alla standardizzazione

Qualora il sistema proposto evolva verso un programma formale di sviluppo o un progetto pilota, dovrà essere allineato agli standard internazionali e ai quadri normativi riconosciuti dalle autorità pubbliche, dall'Unione europea e dagli stakeholder istituzionali.

Tra i principali riferimenti figurano in particolare:

- **ISO/IEC 27001** - gestione della sicurezza delle informazioni,
- **FIDO2** - autenticazione hardware e accesso senza password,
- **Common Criteria EAL5+** o livello equivalente - per dispositivi e chip di sicurezza,
- **eIDAS / eIDAS 2.0** - quadro europeo dell'identità elettronica,
- conformità al **GDPR** e alla normativa nazionale.

II.6 Conclusione principale dell'integrazione sulla sicurezza

La sfida principale di un sistema di questo tipo non riguarda soltanto la tecnologia, bensì la combinazione di:

- conformità giuridica,
- certificazione,
- fiducia istituzionale,
- governance chiara,
- sicurezza dimostrabile.

Il sistema **QEI** può rappresentare un serio concetto di sicurezza soltanto se viene progettato fin dall'inizio come:

- giuridicamente solido,
- tecnicamente decentralizzato,
- operativamente verificabile,
- certificato,
- pienamente tracciabile attraverso audit.

ALLEGATO III - QUADRO OPERATIVO PER L'ULTERIORE ESAME DELL'INIZIATIVA

Per garantire un'efficace prosecuzione dell'esame dell'iniziativa, è opportuno sottolineare che il solo schema, l'idea di base o il materiale di presentazione non sono sufficienti per una valutazione istituzionale. Per una seria valutazione giuridica, tecnica e amministrativa è necessario un documento strutturato che possa essere compreso e valutato da:

- ministeri,
- istituzioni dell'Unione europea,
- autorità di regolamentazione,
- esperti giuridici,
- partner tecnologici,
- autorità di vigilanza.

È pertanto opportuno orientare il lavoro successivo verso i seguenti passaggi operativi.

III.1 Preparazione di un documento formale unitario

È necessario predisporre una versione unica, completa e internamente coerente dell'iniziativa, che contenga almeno:

- titolo e identificazione dell'iniziativa,
- sintesi esecutiva (*Executive Summary*),
- chiara definizione del problema,
- descrizione della soluzione proposta,
- quadro giuridico,
- quadro tecnico,
- scenari concreti di utilizzo,
- meccanismi di sicurezza,
- proposta dei passi successivi.

Tale documento deve essere idoneo alla presentazione formale alle autorità competenti e non deve rimanere soltanto a livello di esposizione concettuale.

III.2 Integrazione e validazione giuridica

Prima di un ulteriore utilizzo del documento nella comunicazione con le istituzioni, è opportuno effettuare un ulteriore allineamento giuridico e definire chiaramente:

- le basi giuridiche ai sensi dell'articolo 6 del GDPR,
- le basi giuridiche ai sensi dell'articolo 9 del GDPR,
- il rapporto tra consenso e interesse pubblico,
- il ruolo del titolare e del responsabile del trattamento,
- il regime della cancellazione, della revoca e dei diritti dell'interessato,
- la questione del controllo giudiziario,
- il rapporto con **eIDAS** e con eventuali futuri quadri normativi europei.

Una tale validazione giuridica aumenterebbe significativamente la serietà e la credibilità dell'iniziativa.

III.3 Concentrazione sul contenuto dell'obiettivo principale

Ai fini dell'accettabilità istituzionale, è particolarmente importante che anche nelle fasi successive l'iniziativa rimanga focalizzata sul proprio contenuto essenziale.

Il nucleo del documento deve rimanere chiaro e comprensibile:

- protezione dei bambini,
- identificazione nei casi eccezionali e particolarmente delicati,
- assenza di una banca dati centrale,
- rigorosa limitazione giuridica dell'utilizzo,
- elevato livello di tutela della privacy.

Le funzionalità aggiuntive possono rimanere come possibili sviluppi futuri, ma non devono offuscare l'obiettivo fondamentale dell'iniziativa.

III.4 Individuazione dei destinatari competenti

Per il successivo esame dell'iniziativa è importante che il documento venga presentato a istituzioni chiaramente individuate e non in modo generico o indeterminato.

Tra i potenziali destinatari competenti figurano in particolare:

- **Commissione europea - Direzione Generale per la Giustizia e i Consumatori (DG JUST)**,
- **Commissione europea - Direzione Generale per la Migrazione e gli Affari Interni (DG HOME)**,
- **Ministero dell'Interno della Repubblica di Slovenia**,
- **Ministero della Giustizia della Repubblica di Slovenia**,
- **Commissario per l'Informazione della Repubblica di Slovenia**,
- **Difensore civico della Repubblica di Slovenia**,
- **Commissioni competenti dell'Assemblea nazionale della Repubblica di Slovenia**,
- altri organi competenti in relazione ai contenuti delle singole fasi dell’iniziativa.

L'individuazione chiara dei destinatari contribuisce a una maggiore serietà procedurale e a un migliore orientamento della comunicazione successiva.

III.5 Presentazione dell'iniziativa come documento ufficiale

L'iniziativa dovrebbe essere presentata alle autorità competenti come un documento unico, strutturato e armonizzato sotto il profilo giuridico e tecnico.

La comunicazione successiva dovrebbe basarsi su una versione unitaria del testo che definisca chiaramente:

- lo scopo dell'iniziativa,
- il quadro giuridico,
- la progettazione tecnica,
- le garanzie contro gli abusi,
- il valore istituzionale,
- i successivi passi proposti.

Un simile approccio è nettamente preferibile rispetto a una presentazione frammentaria o continuamente modificata delle singole parti dell'idea.

III.6 Orientamento operativo conclusivo

Il passo successivo fondamentale non consiste semplicemente nel continuare ad ampliare l'idea, bensì nel consolidarla in un documento sufficientemente chiaro, completo e tecnicamente fondato da poter essere sottoposto a un esame formale.

Da un punto di vista operativo è quindi più opportuno:

- predisporre la versione finale concordata dell'iniziativa,
- effettuare una validazione giuridica e tecnica di base,
- individuare i primi destinatari istituzionali,
- presentare il documento come iniziativa ufficiale per l'avvio di un dibattito tecnico e pubblico.

Un simile approccio garantisce una base strutturata per il dialogo con le autorità nazionali, le istituzioni dell'Unione europea, la comunità accademica e gli altri soggetti interessati, preservando al contempo gli obiettivi fondamentali dell'iniziativa, la sua conformità giuridica e la sua completezza tecnica.

ISTITUTO 1. APRILE

Ricerca • Innovazione • Tecnologie avanzate

REPUBBLICA DI SLOVENIA
GOVERNO DELLA REPUBBLICA DI SLOVENIA

SISTEMA DI IDENTITÀ E AIUTO UMANITARIO QUANTIZZATO (QHIAS)

IDENTITÀ DIGITALE PER L'ACCESSO ALL'AIUTO UMANITARIO PER RIFUGIATI, MIGRANTI E ALTRI GRUPPI VULNERABILI

PROGETTO DI RICERCA PROPOSTO PER LA REPUBBLICA DI SLOVENIA E L'UNIONE EUROPEA – PER UN'EUROPA SICURA, UMANA E DIGITALE

QHIAS è un sistema sicuro di identità digitale e di aiuto umanitario, denominato così in onore della liberazione all'accesso dei servizi essenziali, dell'aiuto e della protezione senza memorizzazione centralizzata dei dati biometrici.



CARATTERISTICHE PRINCIPALI:

- Identificazione sicura senza memorizzazione dei dati biometrici
- Accesso all'aiuto umanitario e ai servizi essenziali
- Prevenzione degli abusi e creazione di identità multiple
- Protezione dei bambini senza accompagnamento
- Conformità al GDPR e ai diritti umani
- Monitoraggio e utilizzo efficace delle risorse pubbliche

PORTAFOGLIO DIGITALE

ACCESSO AI SERVIZI E ALL'ASSISTENZA ESSENZIALI

Distribuzione sicura dei fondi e dei voucher per cibo, alloggio, assistenza sanitaria, istruzione e altro ancora.

AIUTO UMANITARIO

CIBO, ALLOGGIO, ASSISTENZA SANITARIA, ISTRUZIONE

Aiuto mirato e trasparente in base alle reali necessità nelle aree umanitarie più vulnerabili.

PROTEZIONE DEI BAMBINI SENZA ACCOMPAGNAMENTO

IDENTIFICAZIONE E PROTEZIONE MIGLIORE DEI BAMBINI VULNERABILI

Rilevamento precoce e protezione dei bambini senza accompagnatore e prevenzione dei loro abusi.

SICUREZZA E SOVRANITÀ

SICUREZZA SENZA CONTROLLO ECCESSIVO SUI DATI PERSONALI

Maggior fiducia, protezione dei diritti umani e controllo dei dati in conformità con la sovranità nazionale.

IDENTITÀ. PROTEZIONE. AIUTO. DIGNITÀ. UMANITÀ.

DIGNITÀ UMANA · SOVRANITÀ DEI DATI · SICUREZZA · TRASPARENZA · RESPONSABILITÀ · SOLIDARIETÀ

GDPR CONFORME

Il progetto è conforme al GDPR, al diritto dell'UE e agli standard internazionali in materia di diritti umani.

Proponente: Istituto 1. aprile | Izola, Slovenia | 2026 | institut1april.com

ALLEGATO IV - SISTEMA QEI PER L'IDENTITÀ E L'ASSISTENZA UMANITARIA (QHIAS)

POSSIBILE APPLICAZIONE AGGIUNTIVA DELLA TECNOLOGIA QEI PER LA PROTEZIONE DI RIFUGIATI, MIGRANTI E DI ALTRI GRUPPI VULNERABILI

IV.1 Introduzione

Negli ultimi decenni, l'Unione europea si trova ad affrontare flussi migratori sempre più consistenti, crisi umanitarie, guerre, calamità naturali e casi di tratta di esseri umani.

Tra i gruppi particolarmente vulnerabili rientrano:

- minori non accompagnati,
- persone prive di documenti di identità,
- rifugiati,
- migranti,
- vittime della tratta di esseri umani,
- persone che, a causa di guerre o calamità, perdono la possibilità di dimostrare la propria identità.

Lo scopo del presente allegato è presentare il possibile impiego del sistema **QHIAS (QEI Humanitarian Identity & Aid System)** quale quadro di identità umanitaria che potrebbe contribuire alla tutela dei diritti fondamentali, facilitare una verifica dell'identità sicura e affidabile e sostenere un'erogazione trasparente degli aiuti umanitari, nel pieno rispetto del diritto alla privacy e delle garanzie giuridiche vigenti.

IV.2 Finalità del sistema

Il sistema **QHIAS (QEI Humanitarian Identity & Aid System)** è concepito come un sistema volontario, orientato alla tutela della privacy e tecnologicamente avanzato, destinato a sostenere i programmi umanitari.

I suoi obiettivi comprendono:

- protezione dei minori non accompagnati,
- protezione dei rifugiati e dei migranti,
- prevenzione della tratta di esseri umani,
- prevenzione del furto d'identità,
- riduzione degli abusi nei sistemi umanitari,
- identificazione più rapida delle persone prive di documenti,
- accesso più efficiente ai servizi sociali e sanitari,
- gestione più trasparente degli aiuti umanitari.

IV.3 Identità digitale umanitaria

Ogni beneficiario potrebbe ricevere:

- una chiave di identificazione **QEI**,

- una carta di identificazione NFC,
- un identificatore QR,
- un'identità digitale,
- un PIN personale di sicurezza.

L'identità si basa su un token **QEI** protetto crittograficamente e non contiene dati biometrici grezzi.

Il sistema non crea una banca dati biometrica centralizzata e non consente la sorveglianza di massa della popolazione.

L'accesso all'identità è possibile esclusivamente nell'ambito della legislazione vigente, delle procedure previste e sotto adeguato controllo.

IV.4 Portafoglio digitale umanitario

Il quadro **QHIAS** può comprendere un portafoglio digitale umanitario progettato per sostenere un'erogazione degli aiuti sicura, trasparente e responsabile.

Il suo utilizzo potrebbe consentire:

- buoni alimentari,
- trasferimenti umanitari,
- assistenza sociale,
- accesso ai servizi sanitari,
- programmi educativi,
- sostegno all'alloggio,
- assistenza d'emergenza in situazioni di crisi.

Le risorse potrebbero essere fornite da:

- Unione europea,
- Stati membri,
- organizzazioni internazionali,
- organizzazioni umanitarie,
- programmi pubblici di assistenza.

Il sistema consente la tracciabilità dei fondi pubblici e riduce il rischio di abusi.

IV.5 Protezione dei minori non accompagnati

Particolare attenzione è dedicata alla protezione dei minori non accompagnati, che rappresentano uno dei gruppi più vulnerabili nei contesti umanitari e migratori.

Il sistema può contribuire a:

- identificare più rapidamente il minore,
- proteggerlo dalla tratta di minori,
- prevenire le adozioni illegali,
- proteggerlo dallo sfruttamento,
- favorire il ricongiungimento familiare,
- tutelare i minori nei centri di accoglienza per rifugiati.

Lo scopo del sistema proposto non è monitorare o tracciare i bambini, bensì rafforzarne la protezione, tutelarne i diritti e sostenere le autorità competenti e le organizzazioni umanitarie nell'agire nel superiore interesse del minore, conformemente agli standard giuridici vigenti e ai principi dei diritti umani.

IV.6 Prevenzione della tratta di esseri umani

La tratta di esseri umani continua a rappresentare una delle più gravi minacce per le persone vulnerabili, in particolare per i bambini, i rifugiati, i migranti e le altre persone esposte al rischio di sfruttamento.

Il quadro **QHIAS** proposto può fungere da meccanismo di protezione complementare a supporto dell'individuazione e della prevenzione di:

- tratta di esseri umani,
- sfruttamento sessuale,
- lavoro forzato,
- criminalità organizzata,
- reti di migrazione illegale.

Il sistema proposto non è destinato a sostituire le procedure di perseguimento penale o le indagini giudiziarie. È invece concepito per integrare i meccanismi giuridici e istituzionali esistenti, sostenendo una verifica sicura dell'identità in circostanze rigorosamente definite dalla legge e nel pieno rispetto della normativa vigente e dei diritti fondamentali.

IV.7 Garanzie giuridiche ed etiche

Il quadro **QHIAS** proposto dovrebbe basarsi sui seguenti principi:

- rispetto dei diritti umani,
- rispetto del GDPR,
- principio di **Privacy by Design**,
- principio di **Data Minimization**,
- principio di **Purpose Limitation**,
- divieto di discriminazione,
- divieto di utilizzo politico,
- divieto di sorveglianza di massa,
- completa tracciabilità di audit.

Il sistema non deve consentire:

- profilazione politica,
- profilazione religiosa,
- monitoraggio della posizione geografica delle persone,
- utilizzo commerciale dei dati,
- processi decisionali automatizzati senza controllo umano.

IV.8 Distribuzione intelligente degli aiuti

In futuro il sistema potrebbe consentire:

- una distribuzione più rapida degli aiuti,
- la prevenzione dei pagamenti duplicati,
- la riduzione dei costi amministrativi,
- un migliore controllo dell'utilizzo dei fondi pubblici,
- un'assistenza più efficace in caso di calamità naturali,
- un'assistenza più efficace in caso di guerre e crisi.

Qualsiasi futura implementazione di tali funzionalità dovrà rimanere soggetta alle garanzie giuridiche vigenti, a un adeguato controllo istituzionale e ai principi fondamentali di trasparenza, proporzionalità e tutela dei diritti fondamentali.

IV.9 Identità digitale per le persone prive di documenti

Molte persone perdono i propri documenti d'identità a causa di conflitti armati, calamità naturali, crisi umanitarie o sfollamenti forzati.

Il quadro **QHIAS** proposto potrebbe supportare il rilascio di un'identità digitale umanitaria temporanea per facilitare l'accesso a:

- assistenza sanitaria di base,
- aiuti umanitari,
- programmi sociali,
- istruzione,
- assistenza legale.

Tale identità digitale umanitaria non è destinata a sostituire la cittadinanza, la nazionalità, la residenza legale o qualsiasi altro status civile giuridicamente riconosciuto.

Essa è invece concepita per garantire un accesso temporaneo e sicuro ai servizi essenziali, mentre l'identità giuridica o lo status della persona vengono accertati o verificati conformemente al diritto nazionale vigente, al diritto dell'Unione europea e al diritto internazionale.

IV.10 Possibile collegamento con l'identità digitale europea

Poiché l'ecosistema europeo dell'identità digitale è in continua evoluzione, potrebbe essere valutata l'interoperabilità del quadro **QHIAS** proposto con le infrastrutture europee di identità esistenti e future.

I possibili ambiti di interoperabilità comprendono:

- **eIDAS 2.0**,
- **Portafoglio Europeo di Identità Digitale (EUDI Wallet)**,
- identificatori decentralizzati (**DID**),
- credenziali verificabili (**VC**).

Tale collegamento dovrà sempre rispettare:

- gli ordinamenti costituzionali nazionali,
- la legislazione dell'Unione europea,
- la normativa vigente in materia di protezione dei dati e della privacy,
- i principi di necessità, proporzionalità e limitazione della finalità.

Qualsiasi forma di interoperabilità dovrà essere presa in considerazione esclusivamente se favorisce gli obiettivi umanitari del sistema e non compromette la privacy, la sicurezza o i diritti fondamentali delle persone interessate.

IV.11 Progetto pilota dell'Unione europea

Per valutare la fattibilità e i potenziali benefici del quadro **QHIAS** in un ambiente controllato e conforme alla legge, potrebbe essere preso in considerazione un progetto pilota su base volontaria.

Possibili partner:

- Commissione europea,
- UNICEF,
- Alto Commissariato delle Nazioni Unite per i Rifugiati (**UNHCR**),
- Agenzia dell'Unione europea per l'asilo (**EUAA**),
- Agenzia europea della guardia di frontiera e costiera (**Frontex**),
- Stati membri dell'Unione europea.

Gli obiettivi del progetto pilota potrebbero comprendere:

- valutazione della fattibilità tecnica del quadro proposto,
- valutazione della conformità ai requisiti giuridici e normativi vigenti,
- valutazione dei costi di implementazione e gestione,
- valutazione del possibile impatto sui diritti fondamentali e sulla protezione dei dati,
- valutazione dei possibili benefici per la protezione delle persone vulnerabili, in particolare bambini, rifugiati, migranti e vittime della tratta di esseri umani.

Qualsiasi progetto pilota dovrebbe essere realizzato esclusivamente su base volontaria, sotto controllo indipendente e nel pieno rispetto della legislazione nazionale vigente, del diritto dell'Unione europea e degli standard internazionali in materia di diritti umani.

IV.12 Conclusione

Il sistema **QEI Humanitarian Identity & Aid System (QHIAS)** rappresenta una possibile applicazione umanitaria del quadro **QEI**, progettata per sostenere la protezione di rifugiati, migranti, minori non accompagnati e altre persone vulnerabili.

Lo scopo del sistema proposto non è consentire la sorveglianza della popolazione, bensì rafforzare la tutela dei diritti fondamentali, migliorare un'erogazione sicura e trasparente degli aiuti umanitari, contribuire alla prevenzione della tratta di esseri umani e fornire un quadro di identità digitale rispettoso della privacy per finalità umanitarie.

Qualsiasi futura valutazione, sviluppo o implementazione del quadro proposto dovrà basarsi su una valutazione completa sotto il profilo giuridico, tecnico, etico e operativo e dovrà essere conforme ai più elevati standard di tutela dei diritti umani, della privacy, della protezione dei dati, della sicurezza e della responsabilità istituzionale.

Il quadro proposto dovrebbe essere considerato una base per un ulteriore dibattito tecnico e per una successiva valutazione, e non come una proposta di immediata attuazione. Qualsiasi futuro utilizzo dovrà essere subordinato alla partecipazione volontaria, al controllo democratico e alla piena conformità con i quadri giuridici nazionali vigenti, con il diritto dell'Unione europea e con il diritto internazionale.

ALLEGATO V - ARCHITETTURA TECNICA E MODELLO DI SVILUPPO FUTURO DEL SISTEMA QEI

INTEGRAZIONE TECNICA AGGIUNTIVA PER L'ULTERIORE SVILUPPO DELL'IDENTITÀ DIGITALE, DELL'AUTENTICAZIONE CRITTOGRAFICA E DEI SISTEMI DI IDENTITÀ DECENTRALIZZATI

V.1 Scopo dell'allegato

Lo scopo del presente allegato è presentare le possibili linee guida tecniche per il futuro sviluppo del quadro **QEI (Quantized Encrypted Identity)** e delineare le possibili implementazioni di un'architettura avanzata dell'identità digitale che integri biometria, crittografia, tecnologie di identità decentralizzata e moderni meccanismi di sicurezza.

Il presente allegato non costituisce una specifica tecnica definitiva. Esso fornisce invece un quadro di riferimento per la ricerca e lo sviluppo, destinato a sostenere ulteriori valutazioni tecniche, analisi specialistiche, progetti pilota ed eventuali future implementazioni a livello nazionale, europeo o internazionale.

V.2 Modello biometrico multifattoriale

Il quadro **QEI** proposto si basa sul concetto di combinazione di più fattori biometrici indipendenti al fine di garantire un elevato livello di affidabilità, sicurezza e resilienza.

I possibili fattori biometrici comprendono:

- impronta digitale,
- biometria facciale,
- impronta vocale,
- iride,
- geometria del volto,
- marcatori cutanei,
- nei,
- cicatrici,
- tatuaggi,
- altre caratteristiche biometriche consentite,
- marcatori STR trasformati (opzionali).

Ogni fattore biometrico viene convertito in un modello biometrico standardizzato prima di qualsiasi elaborazione crittografica.

Il quadro proposto non utilizza i dati biometrici grezzi come identificatore dell'identità. Al contrario, i dati biometrici fungono esclusivamente da input locale per la generazione di materiale crittografico, nel rispetto dei principi di minimizzazione dei dati, **Privacy by Design** e verifica sicura dell'identità.

V.3 Stabilizzazione dei dati biometrici

Poiché le acquisizioni biometriche possono naturalmente variare tra un tentativo di autenticazione e l'altro, il quadro **QEI** proposto incorpora ulteriori meccanismi di stabilizzazione per garantire un'elaborazione crittografica coerente e affidabile.

Tali meccanismi possono comprendere:

- **Fuzzy Extractor**,
- codici di correzione degli errori (**ECC**),
- metodi di quantizzazione,
- normalizzazione delle caratteristiche,
- stabilizzazione del modello biometrico.

Esempi:

Tabella: Fattore biometrico e rappresentazione standardizzata:

Fattore biometrico	**Rappresentazione standardizzata**
Impronta digitale	Feature Vector
Volto	Embedding Vector
Voce	Voice Embedding
Tatuaggio	Texture Descriptor

Nota: *La rappresentazione standardizzata è una rappresentazione tecnica di una caratteristica biometrica che non coincide con il dato biometrico grezzo.*

Dopo il processo di stabilizzazione, il sistema deriva da ciascun fattore biometrico il corrispondente materiale crittografico.

K_FP

K_FACE

K_VOICE

K_BODY

Questi valori rappresentano materiale crittografico derivato da modelli biometrici standardizzati e non direttamente dai dati biometrici.

Questo approccio consente al sistema di generare lo stesso risultato crittografico, o un risultato sufficientemente coerente, a partire da acquisizioni biometriche naturalmente leggermente diverse, rendendolo idoneo per un utilizzo successivo. In questo modo garantisce un'autenticazione affidabile, mantenendo al contempo un elevato livello di tutela della privacy e di sicurezza delle informazioni biometriche.

V.4 Generazione dell'identità crittografica

La chiave crittografica finale di identificazione viene generata combinando più fattori biometrici e di sicurezza tra loro indipendenti.

Esempio:

K_FINAL = HKDF(
K_FP || K_FACE || K_BODY || SALT || CTX

Dove:

- **K_FP** = materiale crittografico derivato dall'impronta digitale;
- **K_FACE** = materiale crittografico derivato dalla biometria facciale;
- **K_BODY** = materiale crittografico derivato da marcatori corporei, quali nei, cicatrici o tatuaggi;
- **SALT** = parametro di sicurezza casuale che garantisce unicità e resistenza agli attacchi precomputati;
- **CTX (Context)** = contesto di utilizzo associato a uno specifico scopo o ambiente, che impedisce la correlazione dei risultati tra sistemi o casi d'uso differenti.

Questo approccio consente alla chiave crittografica finale di non dipendere da un unico fattore biometrico, ma di rappresentare il risultato della combinazione sicura di più input indipendenti insieme ad ulteriori elementi di sicurezza crittografica.

Dalla chiave così ottenuta viene generato:

QEI_TOKEN = SHA3-512(
K_FINAL || CTX
)

QEI Token:

- non contiene dati personali;
- non contiene dati biometrici;
- non consente la ricostruzione dell'identità;
- non consente la ricostruzione dei dati biometrici;
- non contiene informazioni sanitarie o genetiche.

Il **QEI Token** funge esclusivamente da identificatore crittografico anonimizzato ed è destinato unicamente alla verifica dell'identità nell'ambito di procedure legalmente autorizzate e rigorosamente controllate. Di per sé non rivela né rappresenta l'identità della persona.

V.5 Elaborazione locale e moduli sicuri

Tutti i dati biometrici vengono elaborati esclusivamente in locale.

Gli ambienti supportati possono comprendere:

- **Trusted Execution Environment (TEE),**
- **Secure Enclave,**
- **Secure Element,**
- **StrongBox,**
- **Hardware Security Module (HSM),**
- altri moduli di sicurezza certificati.

I dati biometrici non lasciano mai il dispositivo in forma grezza o ricostruibile.

Il server riceve esclusivamente:

- **QEI Token**,
- la chiave pubblica,
- risultati firmati crittograficamente.

Questa architettura riduce significativamente il rischio di furto dei dati biometrici, di violazioni massive dei dati e di utilizzo non autorizzato su larga scala, garantendo che i dati biometrici sensibili rimangano confinati all'interno di ambienti locali affidabili per l'elaborazione.

V.6 Autenticazione crittografica

Il sistema utilizza il meccanismo **Challenge-Response**.

Procedura:

- il server invia una sfida crittografica;
- il dispositivo genera o sblocca localmente **K_FINAL**;
- il dispositivo crea una firma digitale;
- il server verifica la firma.

Il sistema non trasmette mai:

- dati biometrici grezzi;
- modelli biometrici;
- dati genetici;
- dati personali.

Il risultato può essere:

- accesso autorizzato;
- accesso negato;
- richiesta di un fattore aggiuntivo.

Questa architettura garantisce un elevato livello di tutela della privacy e della sicurezza.

V.7 Identità digitale decentralizzata

Il framework **QEI** è progettato per supportare l'interoperabilità con gli ecosistemi di identità digitale decentralizzata e con i moderni standard per la verifica dell'identità e lo scambio di credenziali digitali.

Flusso concettuale illustrativo:

Biometria

↓

QEI

↓

Coppia di chiavi Ed25519

↓

Identità Digitale W3C DID

La potenziale interoperabilità comprende:

- **W3C DID** (Identificatori Decentralizzati);
- **Verifiable Credentials (VC)**;
- **Hyperledger Foundation**;
- progetti di identità digitale della **Linux Foundation**;
- **eIDAS 2.0**;
- **Portafoglio Europeo di Identità Digitale (EUDI Wallet)**.

Questo approccio consente di creare un'identità digitale senza dipendere da password, documenti di identificazione fisici o banche dati centralizzate.

L'individuo rimane il principale titolare e gestore della propria identità digitale, mantenendo il controllo sull'utilizzo e sulla divulgazione delle proprie credenziali digitali nel rispetto della normativa vigente e dei principi di tutela della privacy.

V.8 Possibili prodotti e ambiti di applicazione

Sulla base del sistema **QEI** è possibile sviluppare diverse soluzioni.

Carta QEI

Carta intelligente dotata di un elemento di sicurezza.

Possibili applicazioni:

- identità elettronica,
- sistemi sanitari,
- pubblica amministrazione,
- settore bancario.

Applicazione mobile QEI

Applicazione mobile per l'identità digitale senza utilizzo di password.

Esempio di utilizzo:

Riconoscimento facciale + impronta digitale = identità digitale

Sistema QEI per il controllo delle frontiere

Sistema avanzato di identificazione ai valichi di frontiera.

Sistema umanitario QEI

Identità digitale per rifugiati, migranti e programmi umanitari.

Sistema QEI per la protezione dei bambini

Protezione dei bambini, delle persone scomparse e prevenzione della tratta di esseri umani.

Cassaforte sicura QEI

Protezione di:

- beni digitali,
- portafogli di criptovalute,
- documenti sensibili,
- segreti aziendali.

Sistema QEI per i cittadini

Futura identità digitale per i cittadini.

Sistema sanitario QEI

Identità sicura per i sistemi sanitari e la documentazione sanitaria.

V.9 Gestione del ciclo di vita dell'identità

Uno dei principali vantaggi del framework **QEI** è la capacità di rigenerare il materiale crittografico dell'identità senza richiedere alcuna modifica delle caratteristiche biologiche della persona.

Procedura:

- viene generato un nuovo **SALT**;
- viene definito un nuovo **CTX**;
- viene eseguita una nuova trasformazione;
- viene generato un nuovo **QEI Token**;
- il precedente materiale identificativo viene disattivato.

Questo approccio consente al framework di ripristinare la sicurezza dopo la perdita, il furto o la compromissione del materiale crittografico associato all'identità, senza richiedere nuove caratteristiche biometriche.

Rispetto ai sistemi biometrici di identificazione convenzionali, questa capacità rappresenta un importante vantaggio in termini di sicurezza, poiché consente un ripristino sicuro dell'identità mantenendo inalterate le caratteristiche biometriche della persona.

V.10 Vantaggi di sicurezza dell'architettura

L'architettura **QEI** proposta combina diversi meccanismi di sicurezza complementari, tra cui:

- biometria multifattoriale,
- elaborazione locale,
- tokenizzazione crittografica,
- identità decentralizzate,
- possibilità di revoca e rigenerazione,
- assenza di una banca dati biometrica centralizzata,
- elevato livello di tutela della privacy.

L'architettura è progettata in conformità ai seguenti principi internazionalmente riconosciuti in materia di sicurezza e privacy:

- **Privacy by Design** - tutela della privacy fin dalla progettazione del sistema;
- **Privacy by Default** - tutela della privacy come impostazione predefinita;
- **Data Minimization** - principio della minimizzazione dei dati;
- **Purpose Limitation** - principio della limitazione della finalità del trattamento;
- **Security by Design** - sicurezza integrata fin dalla progettazione del sistema;
- **Zero Trust Principles** - principi dell'architettura Zero Trust.

Questo modello architetturale riduce i rischi associati ai repository centralizzati di dati, aumenta la resilienza agli attacchi informatici e rafforza la protezione dei dati personali e biometrici grazie all'elaborazione decentralizzata e ai meccanismi di protezione crittografica.

V.11 Potenziale di ricerca e sviluppo

Il quadro proposto **QEI** presenta un potenziale per ulteriori attività di ricerca e sviluppo in un ampio spettro di ambiti applicativi, tra cui:

- identità digitale,
- protezione dei bambini,
- programmi umanitari,
- pubblica amministrazione,
- sanità,
- settore bancario,
- infrastrutture critiche,
- cybersicurezza,
- identità decentralizzate,
- portafogli digitali,
- futuri sistemi europei di identità.

Le possibili linee di ricerca comprendono:

- intelligenza artificiale per la verifica dell'identità;
- crittografia post-quantistica;
- portafogli digitali europei;
- interoperabilità tra Stati;
- protezione delle infrastrutture critiche;
- identità sicure per l'Internet delle Cose (IoT).

Il quadro proposto potrebbe essere ulteriormente sviluppato attraverso programmi europei di ricerca, innovazione e trasformazione digitale, comprese iniziative congiunte che coinvolgano autorità pubbliche, istituti di ricerca, università, partner industriali e istituzioni dell'Unione europea.

V.12 Conclusione

L'innovazione principale del sistema **QEI** non consiste in un singolo fattore biometrico, bensì nella combinazione di:

- molteplici fattori biometrici indipendenti;
- tecnologia **Fuzzy Extractor**;
- elaborazione locale all'interno di un **Trusted Execution Environment (TEE)** o di un ambiente di esecuzione sicuro equivalente;
- tokenizzazione crittografica;
- rigenerazione dell'identità mediante i parametri **SALT** e **CTX**;
- identità digitali decentralizzate;
- moderni meccanismi crittografici.

Una simile architettura rappresenta una possibile base per le future generazioni di identità digitali, combinando un elevato livello di sicurezza, tutela della privacy, interoperabilità e usabilità, e può contribuire allo sviluppo di una società digitale più sicura nell'Unione europea e oltre.



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

QEI INIZIATIVA

PER LA SICUREZZA, I DIRITTI UMANI E LE OPPORTUNITÀ



LA NOSTRA VISIONE

Costruire un mondo in cui ogni individuo è riconosciuto, protetto e abilitato a vivere con dignità – indipendentemente dall'età, dall'origine, dallo status o dalle circostanze.

LA NOSTRA MISSIONE

Con il sistema innovativo Quantized Encrypted Identity (QEI) promuoviamo la protezione di bambini, rifugiati, migranti e tutti i gruppi vulnerabili, e contribuiamo a prevenire il traffico di esseri umani, le violazioni dei diritti umani e promuoviamo un'assistenza umanitaria efficace in tutto il mondo.

I NOSTRI VALORI

- Promozione dei diritti umani e della dignità
- Sicurezza e tutela dei dati personali
- Anonimizzazione e minimizzazione dei dati
- Trasparenza e tutela giuridica
- Innovazione ed eccellenza tecnologica
- Solidarietà e umanità

QEI – IDENTITÀ È OPPORTUNITÀ

PER LE PERSONE. PER LA SOCIETÀ. PER IL MONDO.

PROTEZIONE DEI BAMBINI

Protezione dei bambini senza accompagnamento, ricerca dei minori scomparsi e prevenzione della tratta di esseri umani.

RIFUGIATI E MIGRANTI

Identità sicura e accesso ai servizi essenziali per rifugiati, migranti e altri gruppi vulnerabili.

ASSISTENZA UMANITARIA

Interventi efficaci, consegna controllata e monitoraggio della distribuzione degli aiuti in situazioni umanitarie.

SICUREZZA E SOVRANITÀ

Protezione crittografica, archiviazione locale e accesso senza memorizzazione di dati biometrici grezzi.

COOPERAZIONE GLOBALE

Conformità agli standard europei (eIDAS 2.0, GDPR) e possibilità di interoperabilità globale.

INSIEME COSTRUIAMO UN MONDO IN CUI L'IDENTITÀ È SICURA, NON UN PRIVILEGIO.

Conforme agli standard europei e ai quadri giuridici dell'Unione Europea.

Tecnologia che mette l'essere umano al centro.

Partnership per un futuro migliore e sicuro per tutti noi.

Istituto 1.aprile™

RICERCA • INNOVAZIONE • TECNOLOGIE AVANZATE

L'IDENTITÀ È OPPORTUNITÀ. L'OPPORTUNITÀ È FUTURO.