IDENTITY IS TRUST. TRUST IS THE FOUNDATION.

INSTITUTE 1. APRIL

STRATEGIC INITIATIVE

FOR THE ESTABLISHMENT OF AN ADVANCED BIOMETRIC SYSTEM
FOR CHILD PROTECTION (QEI)



FOR SECURITY. FOR JUSTICE. FOR THE FUTURE.

FOR PEOPLE. FOR SOCIETY. FOR THE WORLD.

Institute 1.april ®

RESEARCH • INNOVATION • ADVANCED TECHNOLOGIES

IZOLA, SLOVENIA | institut1april.com | 2026

QEI INITIATIVE

THE IDENTITY OF THE FUTURE.
FOR PEOPLE. FOR SOCIETY. FOR THE WORLD.

Quantized Encrypted Identity (QEI) is an advanced, voluntary and secure system of digital identity that combines **biometrics, cryptography** and **decentralized identity** technology to provide the highest level of protection for the most vulnerable people worldwide.

CHILD PROTECTION
Finding missing children, protection of unaccompanied minors and prevention of child trafficking.

REFUGEES AND MIGRANTS
Secure identity and access to services for refugees, migrants and other vulnerable groups.

HUMANITARIAN AID
Efficient and transparent distribution of aid and support in humanitarian operations and in the field.

DIGITAL IDENTITY
Advanced digital identity without data storage, without raw biometric data and without central databases.



PRIVACY AND SECURITY
Local storage in secure environments (TEE / Secure Enclave) and strongest level of cryptographic protection.

HUMAN RIGHTS
Respect for human dignity, privacy and security through data minimization and limited data collection.

GLOBAL INTEROPERABILITY
Interoperability with European and international standards (eIDAS 2.0, GDPR) and global interoperability.

PARTNERSHIP
Together we create a world where identity is a right – not a privilege.

QEI – TECHNOLOGY THAT EMPOWERS

ADVANCED BIOMETRICS
Combines biometric factors to ensure the highest level of accuracy and reliability.

CRYPTOGRAPHIC PROTECTION
Advanced cryptographic algorithms ensure the security and integrity of identity.

LOCAL STORAGE
Biometric data is never stored. Identity is securely generated and stored on the user's device.

DECENTRALIZED IDENTITY
Users have full control over their identity, without reliance on centralized databases.

IDENTITY REGENERATION
Ability to generate a new identity if needed without losing access to essential services.

COMPLIANCE AND ETHICS
Compliant with GDPR, eIDAS 2.0 and the highest ethical standards.

OUR COMMITMENT

DIGNITY
Every person deserves respect and fair treatment.

SOLIDARITY
Technology in service of humanity.

JUSTICE
Equal opportunities for everyone, everywhere.

INNOVATION
Advanced solutions for a better world.

SUSTAINABILITY
For future generations and for our planet.

TOGETHER, WE CREATE A WORLD WHERE IDENTITY IS A **RIGHT**,
SECURITY IS A **FOUNDATION** AND ACCESS IS FOR **EVERYONE**.

Institute 1.april™

RESEARCH • INNOVATION • ADVANCED TECHNOLOGIES

TABLE OF CONTENTS

0. STRATEGIC REASON FOR ACTION (WHY NOW) page **8**
0.1 SIMPLIFIED SYSTEM OPERATION OVERVIEW 9

1. INTRODUCTION **9**

2. BACKGROUND AND PURPOSE OF THE INITIATIVE **10**
2.1 Background 10
2.2 Purpose of the Initiative 11

3. FUNDAMENTAL PRINCIPLES OF THE SYSTEM **11**
3.1 Principle of Voluntariness 11
3.2 Principle of Purpose Limitation 11
3.3 Principle of Data Minimization 11
3.4 Principle of Irreversible Tokenization 12
3.5 Principle of Separation of Records 12
3.6 Principle of Judicial and Independent Oversight 12

4. LEGAL AND ETHICAL FRAMEWORK **12**
4.1 Constitutional Framework 12
4.2 European Legal Framework 12
4.3 Ethical Foundations 12
4.4 Proportionality Test 13
4.5 Legal Proportionality Test 13
4.5.1 Legitimate Objective 13
4.5.2 Necessity of the Measure 13
4.5.3 Minimum Intrusion 13
4.5.4 Proportionality in the Strict Sense 14
4.6 Legal Definition of the Use of the Transformed STR Sample 14
4.7 Explicit Prohibition of Misuse 14
4.8 Key Principle of Identity Separation 15
4.9 Legal Clarification: Debunking Myths About Biometric Systems 15
4.9.1 GDPR Does Not Prohibit but Strictly Regulates 15
4.9.2 Key Difference: The System Does Not Use DNA as Data 15
4.9.3 Compliance with the Privacy by Design Principle 16
4.9.4 Constitutional Basis: Child Protection as a Superior Value 16
4.9.5 System as an Exceptional Protection Mechanism, Not a Surveillance System 16
4.9.6 Conclusion of the Legal Clarification 16

5. POSSIBLE IMPLEMENTATION MODEL **17**
5.1 Basic Implementation Model 17
5.2 Institutional Framework 17
5.3 Complementary Nature of the System 17
5.4 Governance and System Operator 17

6. VOLUNTARY ENROLLMENT MODEL **18**
6.1 oluntary Enrollment of Adults 18
6.2 Voluntary Enrollment of Children 18
6.3 Voluntary Enrollment at Birth 18

7. QEI . BIOMETRIC IDENTIFICATION TOKEN page **18**
7.1 Definition 18
7.2 Key Characteristics 19
7.3 What QEI Must Not Contain 19
7.4 Legal Definition of the QEI System 19
7.5 QEI - Physical Emergency Trigger Suite (PET-S) 19
7.5.1 Common Logic (Unified System) 20
7.5.2 QEI Physical Key 20
7.5.3 PET-2: Emergency Card (Child ID) 21
7.5.4 PET-3: Panic Trigger (Device) 22
7.5.5 System Integration 24

8. PROPOSED QEI SYSTEM ARCHITECTURE AND DATA MODEL **24**
8.1 Basic Architecture 24
8.2 Separate Records 25
8.3 Principle of System Operation 25
8.4 Legally Defined System Architecture 26

9. TRILOCK - THREE-FACTOR SECURITY MODEL **26**
9.1 Basic Design 26
9.2 Threshold Usage Model 26
9.3 Key Combination 27
9.4 Key Advantage of the Model 27
9.5 Operation of the QEI Key Mechanism 27
9.6 QEI ONE - Unified Security Key 28

10. STR BIOMETRIC SAMPLE AS AN ADDITIONAL FACTOR **30**
10.1 Proper Role of the STR Component 30
10.2 Processing Procedure 30
10.3 Fundamental Rules 30
10.4 Legal Advantage of This Design 31

11. CRYPTOGRAPHIC AUTHENTICATION **31**
11.1 Challenge-Response Principle 31
11.2 What the System Never Transmits 31
11.3 *Fail-Safe* Principle 31

12. LOCAL PROCESSING AND SECURE MODULES **32**
12.1 Local Processing 32
12.2 Prohibition of Exporting Biometric Data 32
12.3 Local Key Storage 32
12.4 No Central Biometric Database 32

13. USER NOTIFICATION AND USAGE MONITORING **32**
13.1 Principle of Transparency 32
13.2 User Notification 33
13.3 Audit and Accountability 33

14. REVOCATION AND IDENTITY LIFECYCLE MANAGEMENT page **33**
14.1 Revocation 33
14.2 Advantages 33
14.3 Identity Lifecycle Management Without Changing Biological Characteristics 34

15. REGULATORY REQUIREMENTS **34**
15.1 Additional Regulatory Requirements 34

16. SECURITY AND LEGAL SAFEGUARDS **35**

17. FINANCIAL AND DEVELOPMENT FRAMEWORK **35**
17.1 Possible Sources of Funding 35
17.2 Estimated Cost Assessment 35
17.3 Intellectual Property and Patent Protection 35

18. PUBLIC PRESENTATION AND PUBLIC AWARENESS **36**

19. PROPOSED NEXT STEPS **37**
19.1 Strategic Direction for the Next Steps 37
19.2 Proposal for a Pilot Project 38

20. OFFICIAL PROPOSAL TO THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA **38**

21.LEGAL ARGUMENTS FOR FURTHER PROFESSIONAL DISCUSSION **39**
21.1 Extended Legal Arguments 39

22. INDICATIVE STATISTICAL OVERVIEW AND APPENDICES **39**
22.1 Indicative Statistical Overview 39
22.2 Abductions or Unlawful Removal of Newborns from Maternity Hospitals 41
22.3 Global Human Trafficking - Share of Children 41
22.4 Sources for Supplementary Materials / Notes 42

23. CONCLUSION **44**

24. REFERENCES AND BIBLIOGRAPHY **45**
24.1 International Legal Instruments 45
24.2 European Legislation 45
24.3 National Legislation of the Republic of Slovenia 45
24.4 International Standards and Professional Guidelines 45
24.5 Professional Literature 46

25. GLOSSARY OF KEY TERMS, ABBREVIATIONS AND FOREIGN TERMS **47**

ANNEX I - ADDITIONAL PROFESSIONAL SUPPLEMENT:
MISSING KEY ELEMENTS FOR PRACTICAL IMPLEMENTATION **51**
I.1 Root of Trust 51
I.2 Legal Framework (GDPR + eIDAS + National Framework) 51
I.3 Key Management 52
I.4 Standards and Interoperability 52
I.5 Verification Flow 53

I.6 Attacks and Misuse page 53
I.7 Real-World Usage Scenarios 53
I.8 Funding and Governance 54

ANNEX II - ADDITIONAL SECURITY SUPPLEMENT: THREAT MODEL, SECURITY ARCHITECTURE AND CERTIFICATION FRAMEWORK 55
II.1 Fundamental Security Premise 55
II.2 Main Attack Surfaces 55
II.3 Typical Attacks and Proposed Countermeasures 55
II.4 Layered Security Architecture 57
II.5 Certification and Standardization Framework 57
II.6 Key Conclusion of the Security Supplement 58

ANNEX III - OPERATIONAL FRAMEWORK FOR THE FURTHER CONSIDERATION OF THE INITIATIVE 59
III.1 Preparation of a Unified Formal Document 59
III.2 Legal Supplementation and Validation 59
III.3 Content Consolidation of the Core Purpose 60
III.4 Identification of the Competent Recipients 60
III.5 Submission of the Initiative as an Official Document 60
III.6 Final Operational Guidance 61

ANNEX IV - QEI HUMANITARIAN IDENTITY AND ASSISTANCE SYSTEM (QHIAS) 63
IV.1 Introduction 63
IV.2 Purpose of the System 63
IV.3 Humanitarian Digital Identity 63
IV.4 Humanitarian Digital Wallet 64
IV.5 Protection of Unaccompanied Children 64
IV.6 Prevention of Human Trafficking 65
IV.7 Legal and Ethical Safeguards 65
IV.8 Smart Distribution of Humanitarian Aid 66
IV.9 Digital Identity for Persons Without Identity Documents 66
IV.10 Potential Integration with the European Digital Identity 66
IV.11 European Union Pilot Project 67
IV.12 Conclusion 67

ANNEX V - TECHNICAL ARCHITECTURE AND FRAMEWORK FOR THE FUTURE DEVELOPMENT OF QEI 69
V.1 Purpose of the Annex 69
V.2 Multi-Factor Biometric Model 69
V.3 Biometric Data Stabilization 70
V.4 Cryptographic Identity Generation 71
V.5 Local Processing and Secure Modules 71
V.6 Cryptographic Authentication 72
V.7 Decentralized Digital Identity 72
V.8 Potential Products and Areas of Application 73
V.9 Identity Lifecycle Management 74
V.10 Security Advantages of the Architecture 75
V.11 Research and Development Potential 75
V.12 Conclusion 76

SUMMARY

The Institute 1 April presents a strategic initiative for the development of an advanced digital identity system intended to protect children and other particularly vulnerable groups.

The proposed solution introduces the **QEI (Quantized Encrypted Identity)** biometric identification system, based on anonymized and irreversibly transformed biometric data. The system does not store biological samples, genetic records, or raw biometric data; instead, it generates cryptographic identification tokens that enable secure identity verification exclusively upon an appropriate legal basis and under strict supervision.

The solution is designed in accordance with the principles of **privacy by design**, data minimization, purpose limitation, and the separation of records, and complies with the European legal framework, including the **General Data Protection Regulation (GDPR)**, the **Charter of Fundamental Rights of the European Union**, and other relevant standards for the protection of personal data.

The system can make a significant contribution to locating missing children, preventing human trafficking, detecting illegal adoptions, and resolving cases in which identification through existing methods is either impossible or insufficiently reliable.

The proposed solution is based on original technological concepts in the fields of biometrics, cryptography, and digital identity, for which intellectual property protection and patent protection procedures are being pursued.

The establishment of the **Institute 1. april** and the further development of the **QEI** system represent an important step toward creating a secure, ethical, technologically advanced, and privacy-preserving digital identity for the future in the Republic of Slovenia, the European Union, and the broader international community.

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

INITIATIVE FOR PUBLIC CONSULTATION AND THE PREPARATION OF LEGISLATION

BIOMETRIC IDENTIFICATION SYSTEM FOR THE PROTECTION OF CHILDREN (QEI)

Proposed by:

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

Version 1.0 - April 2026

0. STRATEGIC REASON FOR ACTION (WHY NOW)

In recent years, the European Union and its Member States have been facing growing challenges in the field of child protection, particularly in the context of:

- cross-border migration,
- organized crime and human trafficking,
- illegal adoptions,
- digital identity abuse,
- the development of artificial intelligence and deepfake technologies.

Existing identification systems are based primarily on administrative records that are not directly linked to an individual's biological identity, which, in exceptional cases, allows for the manipulation or misuse of identity.

At the same time, the European Union is developing new digital identity frameworks (**eIDAS 2.0**), creating an opportunity to incorporate advanced, privacy-preserving identification mechanisms.

This raises a fundamental question:

Can a State and the European Union develop a system that would:

- improve the protection of children,
- prevent the most serious forms of abuse,
- operate without a central database,
- respect the highest standards of privacy protection?

This initiative provides an answer to that question and proposes that such a system should, at the very least, be examined from professional, legal, and technical perspectives.

0.1 SIMPLIFIED OVERVIEW OF HOW THE SYSTEM OPERATES

For easier understanding, the basic operation of the system can be summarized in four steps:

1. The child (and the parents) voluntarily enroll in the system.
2. An anonymized cryptographic token is generated from minimal biometric inputs.
3. In the event of an incident, a match between the tokens is verified.
4. Identity may be disclosed exclusively on the basis of a legal basis and under appropriate supervision.

The system:

- does not store raw biometric data,
- does not contain a central identity database,
- does not enable general surveillance,
- operates exclusively in exceptional cases.

1. INTRODUCTION

This initiative proposes the launch of a professional and public discussion on the possibility of introducing a voluntary biometric identification system for the protection of children, based on the use of anonymized cryptographic identification tokens (**QEI**).

The sole purpose of the proposed system would be:

- locating missing children,
- preventing child trafficking,
- detecting illegal adoptions,
- verifying biological parentage in cases of justified suspicion of serious criminal offences against children.

The purpose of this initiative is to examine the possibility of establishing a legally strict, technically secure, and constitutionally proportionate system that would operate exclusively in the interest of protecting children while fully respecting:

- the Constitution of the Republic of Slovenia,
- the law of the European Union,
- personal data protection rules,
- the principle of proportionality,
- the principle of the least possible interference with the rights of the individual.

Despite the existing systems for birth registration and personal identification, there are still cases in which a child's identity cannot be reliably verified or has been unlawfully altered. Such gaps may pose a serious risk to the protection of children, particularly in cases of:

- human trafficking,
- illegal adoptions,

- cross-border criminal offences,
- disputes concerning parentage,
- missing children without the possibility of reliable identification.

Existing systems are generally based on administrative records that are not directly linked to biological identity. The proposed QEI system opens the discussion on the possibility of verifying identity based on minimal, anonymized, and irreversibly processed biometric inputs, without storing raw biometric or biological data.

Within the system, biometric data do not constitute identity; rather, they would serve exclusively as a local mechanism for unlocking a cryptographic key or for generating an irreversible identification token within strictly limited procedures.

Recent cross-border cases of child trafficking, identity manipulation, illegal adoptions, and the increasing risks of digital identity abuse demonstrate the need to consider new, privacy-preserving mechanisms for the protection of children. The purpose of this initiative is to proactively open a professional and public discussion on possible solutions before such risks increase further.

Due to the cross-border nature of child trafficking, illegal adoptions, and cases of missing children, this initiative also has potential relevance at the level of the European Union. Any future development could therefore examine interoperability with European frameworks, while strictly respecting personal data protection rules, the principle of subsidiarity, and constitutional limitations.

The technical model presented below is provided at a conceptual level for the purpose of demonstrating feasibility, security principles, and legal safeguards. Detailed implementation would be the subject of further professional, technical, and legal analysis.

If there is a technology capable of saving the life of even one missing child, it is the duty of the State to at least examine its constitutional, legal, and technical feasibility.

2. BACKGROUND AND PURPOSE OF THE INITIATIVE

2.1 Background

This initiative is based on the need to discuss an additional protective mechanism for children, particularly in cases of:

- child trafficking,
- child slavery and sexual exploitation,
- child abduction at birth,
- unlawful or illegal adoptions,
- systemic errors in the registration of parentage,
- cases of missing children without reliable identification.

Although such cases are statistically relatively rare, they involve extremely sensitive and serious criminal offences in which even a single case may constitute an exceptionally grave violation of the child's human rights and dignity.

2.2 Purpose of the Initiative

The purpose of this initiative is to open a professional, legal, technical, and ethical discussion on the possibility of establishing a system that would:

- operate exclusively for the protection of children,
- be voluntary,
- use minimal biometric templates,
- not store biological samples or raw biometric data,
- permit use only on the basis of a strict legal basis,
- be subject to independent oversight,
- prevent any expansion of its intended purpose.

3. FUNDAMENTAL PRINCIPLES OF THE SYSTEM

The proposed system should be based on the following principles.

3.1 Principle of Voluntary Participation

Participation in the system would be possible exclusively on the basis of free, informed, and explicit consent.

3.2 Principle of Purpose Limitation

The system should be used exclusively for the protection of children, in particular for:

- locating missing children,
- preventing child trafficking,
- detecting illegal adoptions,
- verifying biological parentage in cases of legally authorized proceedings.

Its use for any other purposes should be explicitly prohibited, in particular for:

- the general criminal prosecution of adults,
- tax proceedings,
- medical analyses,
- commercial purposes,
- general population surveillance.

3.3 Principle of Data Minimization

The system should not store:

- biological samples after processing,
- raw biometric data,
- the complete genetic profile,
- genetic health data,
- personal data within the QEI token itself.

3.4 Principle of Irreversible Tokenization

The system would use exclusively standardized biometric templates and generate irreversible cryptographic identification tokens from them.

3.5 Principle of Separation of Records

Identity data, biometric templates, and audit data should be stored in strict separation, without a single central database of sensitive data.

3.6 Principle of Judicial and Independent Oversight

Access to data or the initiation of an identification procedure should be possible only on the basis of:

- a legal basis,
- a court order, where required,
- strict audit traceability,
- independent institutional oversight.

4. LEGAL AND ETHICAL FRAMEWORK

The proposed system should be designed in accordance with the following legal and ethical principles.

4.1 Constitutional Framework

- Constitution of the Republic of Slovenia – Article 35: Protection of the Right to Privacy and Personality Rights,
- Constitution of the Republic of Slovenia – Article 56: Special Protection of Children.

4.2 European Legal Framework

- General Data Protection Regulation (**GDPR**), in particular Articles 6 and 9,
- Charter of Fundamental Rights of the European Union – Articles 7 and 8,
- European Convention on Human Rights – Article 8.

4.3 Ethical Principles

The proposed system should adhere to the following principles:

- **privacy by design**,
- **privacy by default**,
- proportionality,
- necessity,
- minimal interference,

- traceability,
- accountability,
- non-linkability between systems,
- prohibition of the secondary use of data.

4.4 Proportionality Test

Any future legislative framework should pass the proportionality test, which includes:

- a legitimate objective - the protection of children,
- the suitability of the measure,
- the necessity of the measure,
- the least possible interference with the rights of the individual.

4.5 Legal Proportionality Test

The proposed system is designed to satisfy the proportionality test in accordance with constitutional and European case law.

4.5.1 Legitimate Objective

The protection of children against serious forms of criminal offences constitutes a constitutionally protected value under **Article 56 of the Constitution of the Republic of Slovenia** and a legitimate objective within the meaning of **European Union law** and the **European Convention on Human Rights**.

4.5.2 Necessity of the Measure

Existing administrative systems do not always provide reliable identification in cases of:

- illegal adoptions,
- child trafficking,
- cross-border cases without appropriate documentation,
- disputes concerning parentage under particularly sensitive circumstances.

The proposed system represents a complementary mechanism for exceptional cases in which less intrusive measures do not provide the same level of effectiveness.

4.5.3 Minimal Interference

The system is designed in such a way that it:

- does not store biometric or genetic data in raw form,
- uses only transformed, standardized, and irreversible templates,
- operates without the direct identification of individuals,
- does not enable general population surveillance,
- discloses identity only under strictly defined legal conditions.

4.5.4 Proportionality in the Strict Sense

The proposed measures are strictly limited:

- to the protection of children,
- to voluntary participation,
- to judicial or legally prescribed oversight,
- to exceptional and particularly sensitive cases.

Because of these limitations, the interference is significantly narrower than that of conventional centralized systems for the processing of biometric data.

4.6 Legal Definition of the Use of a Transformed STR Profile

Within the system, DNA is not used as identification or analytical data, but exclusively as a transformed, irreversible biometric profile that:

- does not enable the direct identification of an individual,
- does not contain health-related or hereditary information,
- is used exclusively as an additional security factor for a high level of assurance.

Accordingly:

- raw DNA data are never stored,
- the biological sample is immediately and irreversibly destroyed after processing,
- the original DNA cannot be reconstructed from the transformed record.

The transformed STR profile:

- is not used for continuous authentication,
- is not used as a primary identifier,
- is not used for medical, diagnostic, or research purposes.

The system does not use DNA for identification purposes in the conventional sense, but exclusively as a transformed, irreversible cryptographic factor that does not permit the disclosure of genetic or health-related information.

4.7 Explicit Prohibition of Misuse

The system must not be used for:

- general population surveillance,
- the criminal prosecution of adults outside the strictly defined scope of child protection,
- tax or administrative proceedings,
- medical analyses,
- genetic research,
- commercial purposes,
- profiling,
- automated decision-making,
- mass surveillance or the secondary use of data.

Any extension of the system's intended purpose beyond the exclusive protection of children in legally prescribed cases must be expressly prohibited and subject to legal sanctions.

4.8 Fundamental Principle of Identity Separation

The system itself does not enable the identification of an individual. Identification is possible exclusively:

- upon a confirmed match of a token or another cryptographic result,
- when the legal requirements have been fulfilled,
- on the basis of a court order or another legally prescribed legal basis,
- with the access recorded in the audit log.

Without the fulfilment of these conditions, the identity remains inaccessible.

4.9 Legal Clarification: Dispelling Myths About Biometric Systems

There is a common misconception in the public sphere that the European legal framework, in particular the **General Data Protection Regulation (GDPR)**, completely prohibits the use of biometric and genetic data. Such an interpretation is incorrect.

4.9.1 The GDPR Does Not Prohibit; It Strictly Regulates

Article 9 of the GDPR provides that biometric and genetic data constitute a special category of personal data, the processing of which is, as a general rule, restricted but not absolutely prohibited.

Processing is permitted where there is:

- the explicit consent of the individual,
- an important public interest,
- an appropriate legal basis,
- a proportionate and necessary measure.

The proposed system is designed precisely on these principles:

- complete voluntariness,
- strict purpose limitation,
- data minimization,
- use exclusively in exceptional cases involving the protection of children.

4.9.2 The Key Difference: The System Does Not Use DNA as Data

Unlike conventional biometric or forensic databases, the proposed model:

- does not store DNA,
- does not retain biological samples,
- does not allow the reconstruction of genetic data,
- does not contain health-related or other sensitive information.

The DNA, or STR component, is used exclusively as a local cryptographic input for generating an irreversible key.

This means that the system:

- does not create a genetic database,
- does not enable identification without a legal basis,
- does not constitute a permanent biological identifier.

4.9.3 Compliance with the Principle of Privacy by Design

The proposed architecture inherently satisfies the key requirements of European law:

- local data processing only (TEE / Secure Enclave),
- separate records without a central database,
- irreversible tokenization,
- prohibition of the secondary use of data,
- complete access traceability.

Such an architecture represents an even higher standard of data protection than that provided by many existing systems.

4.9.4 Constitutional Basis: Protection of Children as a Superior Value

Article 56 of the Constitution of the Republic of Slovenia provides for the special protection of children. This means that the State is not only entitled, but also obliged, to examine measures that may improve the protection of children, provided that such measures are:

- proportionate,
- necessary,
- constitutionally compliant.

4.9.5 The System as an Exceptional Protective Mechanism, Not a Surveillance System

It is important to emphasize that the proposed system:

- is not intended for the general identification of the population,
- is not intended for surveillance or tracking,
- cannot be used without a legal basis,
- operates exclusively in exceptional cases prescribed by law.

It is a specialized protective mechanism for the most serious cases in which existing systems are insufficient.

4.9.6 Conclusion of the Legal Clarification

The claim that the European legal framework completely prohibits such a system is incorrect. On the contrary, with an appropriate design, safeguards, and legal framework, it is possible to develop a solution that:

- respects fundamental rights,
- adheres to the principles of data protection,
- while at the same time making an effective contribution to the protection of children.

Therefore, this initiative does not represent a departure from the existing legal framework, but rather an attempt to enhance it in the direction of greater protection for the most vulnerable.

5. POSSIBLE IMPLEMENTATION MODEL

5.1 Basic Implementation Model

The proposed model could be based on the following elements:

- voluntary submission of biometric inputs by parents and children,
- processing of only minimal biometric templates,
- generation exclusively of a cryptographic identification token,
- prohibition of storing biological samples or raw biometric data,
- activation of procedures exclusively on the basis of legally authorized proceedings,
- independent institutional oversight,
- strict sanctions for misuse.

5.2 Institutional Framework

The possible institutional framework could include:

- **Ministry of the Interior** - system management,
- **Ministry of Health** - collection of biometric inputs upon enrollment,
- **Police and Criminal Investigation Service** - operational use in legally prescribed cases,
- **Information Commissioner** - oversight of personal data protection,
- **Independent Supervisory Authority** - auditing of the system's operation,
- **Courts** - decisions regarding the admissibility of intervention and access.

5.3 Complementary Nature of the System

The proposed system does not introduce a new form of general identification but rather represents an additional, strictly limited protective mechanism for exceptional cases in which existing systems fail.

The system is not intended to replace existing records but to serve as an additional layer of protection for particularly sensitive child protection cases.

5.4 Governance and System Operator

For the operational implementation of the system, it is essential to clearly define the project owner and the governance structure.

A possible basic structure could be:

- **Lead institution:** the State (e.g., the Ministry of the Interior) or a European framework,
- **Professional lead and development partner:** Institute 1 April,
- **Technology partners:** TBD (development, security, infrastructure),
- **Supervisory authority:** an independent institution (e.g., the Information Commissioner).

Such a distribution enables:

- clear accountability,
- institutional legitimacy,
- professional support,
- transparency of governance.

6. VOLUNTARY ENROLLMENT MODEL

6.1 Voluntary Enrollment of Adults

An adult individual may enroll in the system on the basis of written and informed consent.

At any time, the individual should have the right to request the deletion of their data, unless there is another legal basis requiring their retention.

6.2 Voluntary Enrollment of Children

The enrollment of a minor child would be possible on the basis of the consent of the parents or legal guardians.

Upon reaching the age of majority, the individual should have the right to:

- confirm continued participation, or
- request the deletion of their data.

6.3 Voluntary Enrollment at Birth

Parents could be offered the option of enrolling their child in the system at the time of birth.

The decision should be:

- entirely voluntary,
- free from any negative consequences in the event of refusal,
- carried out in accordance with medical standards.

7. QEI - BIOMETRIC IDENTIFICATION TOKEN

7.1 Definition

QEI (Quantized Encrypted Identity) is an anonymized and cryptographically protected identification system that generates an irreversible identification token from standardized biometric templates.

QEI is not personal data in the form of a name, personal identification number, or any other direct identifier, but rather a technical cryptographic linking element that enables the verification of a match when the applicable legal conditions are fulfilled.

7.2 Key Characteristics

The core of the system would consist of:

- biometric templates, not raw data,
- a single QEI token,
- separate records,
- multi-level access,
- an audit trail,
- privacy by design.

7.3 What the QEI Token Must Not Contain

The QEI token must not contain:

- raw fingerprint images,
- facial photographs,
- the complete genetic profile,
- genetic health data,
- free-text information about an individual,
- political, religious, or other sensitive attributes,
- direct personal identifiers.

7.4 Legal Definition of the QEI System

QEI is an anonymous, cryptographically generated identification token created from standardized biometric templates that:

- does not contain personal data,
- does not enable the reconstruction of an individual's identity,
- does not enable the reconstruction of biometric data,
- does not contain health-related, hereditary, or other sensitive information.

The system ensures:

- complete separation of identity data, biometric templates, and audit records,
- the use of one-way cryptographic functions,
- non-linkability between systems,
- multi-level legal and technical access control.

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

For cases in which biometric activation is not possible, is not appropriate, or cannot be carried out in a timely manner, a complementary system of physical triggers without the use of biometrics is also proposed:

QEI – Physical Emergency Trigger Suite (PET-S)

(Three physical activation methods without the use of biometrics.)

7.5.1 Common Logic (Unified System)

All three triggers operate according to the same logic:

- physical activation,
- cryptographic verification,
- generation of an **Emergency Request (ER)**,
- activation of the **ERAP protocol**,
- without the use of biometrics.

7.5.2 PET-1: QEI Physical Security Key



Form:

- USB-C or NFC security key,
- linked to the Family Token.

Activation:

- insert or tap the security key,
- enter the PIN,
- the system initiates an **Emergency Request (ER)**.

Security:

- Secure Element security chip,
- anti-cloning protection,
- linked to the family.

Use:

- parents,
- the police, provided they have the appropriate legal basis and authorized access.

7.5.3 PET-2: Emergency Card (Child ID)



Form:

The card contains:

- a visual fingerprint marker,
- an NFC chip,
- a QEI identifier (**QEI ID**).

Activation:

- someone finds the child,
- scans the card,
- the system verifies the identifier,
- initiates a signal to the competent authority.

Security:

- pseudonymous identifier only,
- no personal data.

Use:

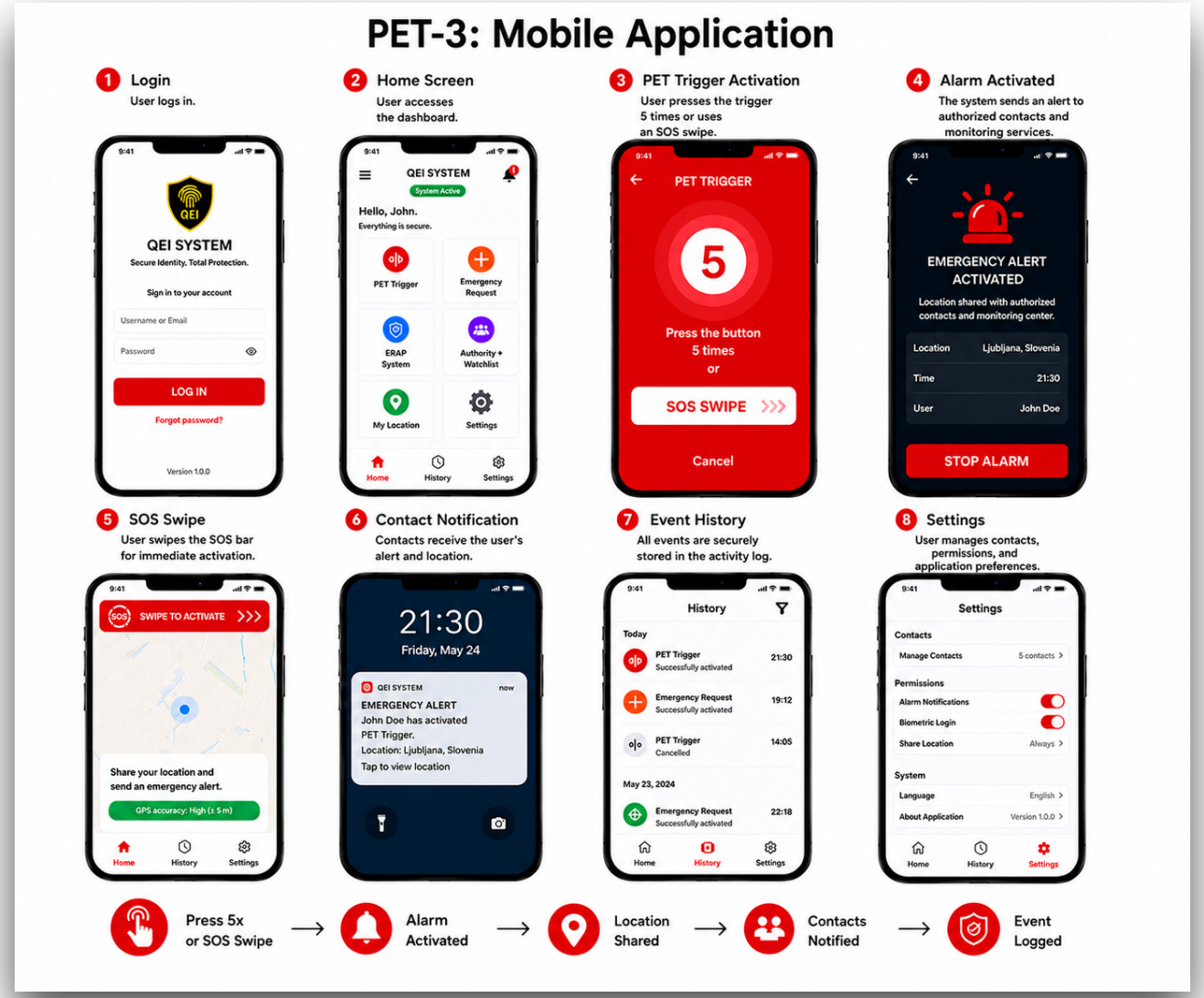
- the public,
- competent authorities.

7.5.4 PET-3: Panic Trigger (Device)

Form:

- a function integrated into a mobile phone or a QEI device.





Activation:

- a hidden activation sequence (e.g., pressing a button five times),
- or an **SOS swipe**.

Security:

- restricted access,
- logging of all activities,
- possibility of cancellation.

Use:

- child,
- parent.

7.5.5 Integration into the System

[PET trigger]

↓

[Emergency Request (ER)]

↓

[ERAP System]

↓

[Competent Authorities + Watchlist Monitoring Services]

8. PROPOSED ARCHITECTURE AND DATA MODEL OF THE QEI SYSTEM

8.1 Basic Architecture

The proposed system would be based on three separate layers.

1. Bio Layer

- biometric templates,
- fingerprint template,
- facial template,
- transformed STR biometric profile.

2. Crypto Layer

- normalization,
- cryptographic transformation,
- generation of the QEI token,
- key derivation,
- digital signature mechanism.

3. Access Layer

- permissions,
- legal basis,
- access auditing,
- role-based access,
- user notification.

8.2 Separate Records

The system should be based on the strict separation of at least three records.

a) Identity Record

A separate external record, which may contain:

- internal identification number,
- first name and surname,
- date of birth,
- nationality,
- person's status,
- contact or guardian information.

The QEI system must not store these data within the cryptographic token.

b) Biometric Record

A separate record of biometric templates, not raw data:

- fingerprint template,
- facial template,
- limited transformed STR template,
- date of capture,
- sample quality,
- source of the sample,
- validity status.

c) QEI Linking Record

This record would contain:

- QEI token,
- technical references linking the records,
- audit records.

8.3 Principle of System Operation

The system would operate according to the following sequence:

- Biometric input → conversion into a template
- Template → generation of a QEI token or cryptographic material
- Token or key material → omparison or digital signature process
- Upon a match → initiation of a legally authorized procedure
- Only then → possible access to the external identity record

8.4 Legally Defined System Architecture

The system is based on three functionally and legally separate layers.

a) Bio Layer

This layer contains exclusively standardized biometric templates and never contains raw biometric or biological data.

b) Crypto Layer

This layer performs cryptographic transformation, tokenization, key derivation, and digital signature processes using one-way and secure cryptographic mechanisms.

c) Access Layer

This layer contains access rules, audit mechanisms, the legal basis for access, judicial oversight, and decision-making mechanisms for determining whether the disclosure of identity is legally permissible.

Such an architecture ensures the functional, technical, and legal separation of the essential components of the system.

9. TRILOCK - THREE-FACTOR SECURITY MODEL

9.1 Basic Design

The most appropriate, secure, and modern implementation of the system is based on the combination of three independent biometric factors, which together form the **TriLock** model:

- **K_STR** - cryptographic material derived from a transformed STR biometric profile,
- **K_FP** - cryptographic material derived from a fingerprint,
- **K_FACE** - cryptographic material derived from facial biometrics.

None of these elements ever leave the device in raw or reconstructable form.

9.2 Threshold Model of Use

The system may employ a multi-level threshold model:

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

Such a model allows the level of assurance to be adapted according to the sensitivity of the individual procedure.

9.3 Key Combination

The final key is generated from multiple factors together with additional system context:

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

The following principles apply:

- HKDF or another comparable secure key derivation mechanism is used,
- each system uses its own **SALT**,
- each purpose of use employs its own **CTX**,
- thereby ensuring non-linkability between systems.

9.4 Key Advantage of the Model

The **TriLock** model provides:

- multi-layered security,
- a significantly lower risk of false matches,
- stronger legal defensibility of the system,
- greater resistance to misuse,
- higher compliance with the principle of data minimization.

9.5 Operation of the QEI Key Mechanism

At the conceptual level, the system operates by having the user activate a local biometric factor, such as a fingerprint, from which a standardized biometric template is generated.

This template is neither stored nor transmitted in raw form; instead, it is used exclusively as a local input for generating a one-time cryptographic signature.

The process operates by the system issuing a **challenge**, after which the device generates a one-time cryptographic response based on the locally verified biometric factors and the system context.

The result may be:

- access granted,
- access denied,
- request for an additional factor.

The key concept of the system is that biometrics do not unlock the system as a static identifier but instead participate in generating a one-time digital key or cryptographic signature.

9.6 QEI ONE - Unified Security Key

Instead of three separate devices, a single physical device may also be envisaged:

QEI ONE - Unified Security Key

Concept

QEI ONE combines:

- a security key (**Token Access**),
- identification (**ID / QR / NFC**),
- **Panic / Emergency Trigger**.

It is a single physical device that combines multiple functions within one unified security carrier.

Appearance:



The **QEI ONE** device may be designed with the following characteristics:

- teardrop-shaped form factor,
- approximately **9 cm** in length,
- approximately **6 cm** in width,
- a slim, ergonomic design.

Functional Layers

Secure Core

- Secure Element (security chip),
- stores fragments of the QEI system and cryptographic material.

NFC + QEI ID

- identification functionality,
- capability to initiate an emergency procedure by scanning (**Emergency Scan**).

SOS Button

- large physical button for initiating an emergency procedure,
- immediately activates the **ERAP** protocol.

LED Indicator

- **green** = system operating normally,
- **red** = Emergency Mode activated,
- **blue** = device is active or connected.

Battery

- compact built-in battery,
- long operating autonomy.

How It Works

Normal Operation

- the device is brought close to a reader,
- NFC enables access.

Emergency Situation

- the **SOS button** is pressed,
- or a fingerprint is used,
- the system initiates the **ERAP** protocol.

Architecture in a Single Device

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

Advantages

- one device,
- simpler operation,
- always with the user,
- enhanced security,
- multiple activation methods,
- not exclusively dependent on biometrics,
- a stronger patent concept based on a **multi-function hardware identity token**.

10. STR BIOMETRIC PROFILE AS AN ADDITIONAL FACTOR

10.1 The Proper Role of the STR Component

Within the system, DNA is not used as a permanent identifier but exclusively as a transformed STR biometric profile from which cryptographic material is generated.

This means that the system is not based on the storage of DNA but on the short-term technical transformation of a limited set of identification markers.

10.2 Processing Procedure

The process may follow the following model:

STR → numerical vector → addition of SALT → transformation → fuzzy extractor → K_STR

or, in greater detail:

STR → normalization → binary representation → addition of SALT + CTX → randomized transformation → fuzzy extractor → generation of cryptographic material K_STR

10.3 Fundamental Principles

- raw DNA data are deleted immediately after processing,
- the complete genetic profile is not stored,
- **K_STR** does not represent the identity of an individual,
- **K_STR** is used exclusively as local cryptographic material,
- the STR component is used only as an additional factor for a high level of assurance.

10.4 Legal Advantage of This Design

This approach moves the system away from the model of **"DNA as data"** and toward the model of **"a transformed biometric factor for local cryptographic use,"** which is significantly more defensible from the perspective of:

- privacy protection,
- the principle of data minimization,
- the principle of **privacy by design**,
- purpose limitation.

11. CRYPTOGRAPHIC AUTHENTICATION

11.1 Challenge-Response Principle

The system should use a **challenge-response** cryptographic mechanism.

The process operates as follows:

1. The server sends a cryptographically secure **challenge**.
2. The device locally generates or unlocks the **K_FINAL** key.
3. The device signs the challenge using the **K_FINAL** key.
4. The server verifies the signature using the corresponding public key.

11.2 What the System Never Transmits

The system never transmits:

- raw biometric data,
- biometric templates,
- an STR profile,
- the token as an identity.

Biometrics and tokens are not used as a direct means of authentication but rather as a local activation mechanism for generating a cryptographic signature.

11.3 *Fail-Safe* Principle

In the event of doubt, error, an incomplete match, or technical uncertainty, the system shall not disclose the identity of the individual.

The system's default behavior must be to deny access or require additional verification rather than disclose identity data.

12. LOCAL PROCESSING AND SECURE MODULES

12.1 Local Processing

The system must ensure that all biometric data are processed exclusively locally within a secure hardware-software environment, such as:

- **Trusted Execution Environment (TEE)**,
- **Secure Enclave**,
- or another comparable secure module.

12.2 Prohibition of Biometric Data Export

Biometric input data:

- must not leave the device in raw form,
- must not leave the device in a reconstructable form,
- must not be used as a global identifier,
- must not be transmitted to central databases.

12.3 Local Storage of Keys

The device must generate and store the private cryptographic key within a secure module.

Server systems must not store biometric data or their direct representations.

12.4 No Central Biometric Database

The system does not establish a centralized database of biometric or genetic data.

Only an anonymized cryptographic token or a minimal technical result is stored, which in itself does not enable the identification of an individual or the reconstruction of biometric data.

13. USER NOTIFICATION AND USAGE OVERSIGHT

13.1 Principle of Transparency of Use

Every use of the system must be recorded in an audit log.

The usage record must include at least:

- time,
- service or procedure,
- location or system source,
- result of the use.

13.2 User Notification

Where legally and operationally permissible, the user must receive notification of the use of their identification mechanism.

If the use was not authorized by an authorized person, the system must enable:

- blocking of further use,
- system reset or replacement of the key material,
- revocation of the existing key,
- initiation of an audit or security procedure.

13.3 Audit and Accountability

The system must ensure complete traceability of all access events and all procedure activations.

The audit record must contain at least:

- who accessed the system,
- when the access occurred,
- on what legal basis,
- for what purpose,
- the outcome of the procedure.

The system must be subject to an independent supervisory mechanism that enables the regular assessment of the legality, proportionality, and security of its use.

14. REVOCATION AND IDENTITY LIFECYCLE MANAGEMENT

14.1 Revocation

In the event of a compromise, the system must allow the replacement of identity material without changing the individual's biological characteristics.

The procedure:

- generate a new **SALT**,
- perform a new transformation of the biometric material,
- generate a new cryptographic key,
- deactivate the previous key.

14.2 Advantage

This means that the system is not static and enables the restoration of security even after an incident, which is one of its key advantages over conventional centralized biometric databases.

14.3 Identity Management Without Changing Biological Characteristics

The system enables the regeneration of identity or cryptographic material without requiring any change to the individual's biological characteristics.

This is achieved by:

- generating a new **SALT**,
- using a new **CTX**, where necessary,
- performing a new cryptographic transformation,
- generating a new key,
- deactivating the previous key.

Such a mechanism significantly reduces the risk of permanent compromise.

15. NORMATIVE REQUIREMENTS

The system should meet at least the following requirements:

- biometric data are processed exclusively locally,
- the STR profile is used only as a transformed and irreversible biometric profile,
- tokens are not identity and are not used for direct authentication,
- authentication is based on a cryptographic signature,
- **SALT** must be unique for each user and each system,
- **CTX** must be linked to the intended purpose,
- the system must support **revocation**,
- a centralized biometric database is not permitted,
- systems must not be cryptographically linkable to one another,
- every intervention must be traceable and legally restricted.

15.1 Additional Normative Requirements

The system must additionally ensure:

- non-linkability of tokens between systems,
- the use of **SALT** at the user level,
- the use of **CTX** at the purpose level,
- multi-factor usage logic,
- prohibition of the use of a token as a direct identity,
- the principle of minimal system response,
- the **fail-safe** principle in the event of an inconclusive result,
- mandatory audit logging of all access events.

16. SECURITY AND LEGAL SAFEGUARDS

The system should include:

- separate and encrypted data storage,
- multi-level encryption,
- access exclusively on the basis of legally authorized procedures,
- an independent supervisory authority,
- annual public reporting,
- regular security penetration testing,
- certification in accordance with information security standards,
- decentralized security mechanisms,
- long-term resilience of cryptographic solutions.

Any misuse or expansion of the system's intended purpose should be subject to legal sanctions.

17. FINANCIAL AND DEVELOPMENT FRAMEWORK

17.1 Possible Sources of Funding

- state budget,
- European programmes,
- research and development projects,
- public-private partnerships, where legally and ethically permissible.

17.2 Indicative Cost Estimate

For the purpose of an initial feasibility assessment, the following indicative financial estimate may be established:

- system development: **EUR 2–5 million**,
- pilot project: approximately **EUR 500,000**,
- annual maintenance: dependent on the scope of implementation.

Possible sources of funding include:

- European programmes (e.g., **Horizon Europe**, **Digital Europe**, **LIFE**),
- national funding,
- combined financing models.

In this context, a high level of co-financing by the European Union (up to **90%**) may be expected, particularly within projects related to digital identity and the protection of vulnerable groups.

17.3 Intellectual Property and Patent Protection

The proposed **QEI (Quantized Encrypted Identity)** system incorporates several original technical, security, and organizational solutions in the fields of biometric identity, cryptography, privacy protection, identity tokenization, and secure digital authentication.

The proponent of this initiative has prepared and/or filed intellectual property and patent protection procedures for individual technical elements of the system with the competent industrial property authorities.

The subject matter of the protection may include, among other things:

- the anonymized biometric identity system **QEI_TOKEN**,
- methods for generating cryptographic material from multiple independent biometric factors,
- the **TriLock** multi-factor security model (**STR + fingerprint + facial biometrics**),
- a system of separate records for identity data, biometric templates, and audit records,
- **QEI ONE** - a multifunctional physical identification and security key,
- **PET-S (Physical Emergency Trigger Suite)** for initiating emergency procedures without the use of biometrics,
- methods for the local processing of biometric data without centralized storage of biometric data,
- methods for irreversible identity tokenization and cryptographic verification.

Patent protection does not restrict public, professional, or legislative discussion of this initiative. Its purpose is to protect innovative solutions, prevent the unauthorized appropriation of intellectual property, and enable the further development of the system in cooperation with government authorities, research institutions, universities, industry, and the institutions of the European Union.

The proponent expresses its willingness to cooperate with the **Republic of Slovenia**, the institutions of the **European Union**, and international organizations in the further professional, legal, and technical assessment of the system.

In the event of further development and possible implementation of the system, an appropriate licensing model, public-private partnership, research cooperation, or another legally permissible technology transfer model may be applied, ensuring the protection of the public interest, human rights, and the protection of children.

All future development activities must be carried out in accordance with the legislation of the **Republic of Slovenia**, the law of the **European Union**, international information security standards, and the principles of personal data protection and privacy.

18. PUBLIC PRESENTATION AND PUBLIC AWARENESS

In the event of further consideration of this initiative, a transparent public presentation of the system should be ensured.

The public presentation should include the participation of:

- constitutional law experts,
- personal data protection specialists,
- bioethicists,
- representatives of civil society,
- child protection experts,
- information technology and cryptography experts.

Particular emphasis should be placed on explaining:

- the strict limitation of purpose,
- the technical and security safeguards,
- the voluntary nature of participation,
- the possibility of data deletion,
- judicial and independent oversight.

The system must not be presented as a general surveillance mechanism but exclusively as a specialized protective instrument for the protection of children.

19. PROPOSED NEXT STEPS

We propose:

- organizing a public consultation at the national level,
- preparing a professional analysis of constitutional compliance,
- preparing an assessment of compliance with the GDPR and European Union law,
- preparing a technical feasibility study,
- involving domestic and international experts,
- examining the possibility of a pilot model, if legally permissible,
- continuing the discussion on the potential European dimension of the initiative.

Should the implementation in the Republic of Slovenia prove successful, the initiative could subsequently be presented at the level of the European Union and later as a broader international initiative for the protection of children.

19.1 Strategic Direction for Further Steps

For the successful further consideration of this initiative, it is important to emphasize that the objective is not the immediate implementation of the system without prior assessment, but rather:

- professional analysis,
- legal validation,
- technical feasibility study,
- a pilot model, if legally permissible.

The strongest approach is not **"let us implement the system,"** but rather **"let us examine the system as a complementary protective mechanism for exceptional cases."**

Such an approach:

- reduces resistance,
- increases legal acceptability,
- enables institutional support,
- opens the possibility of funding at the level of the European Union.

The primary purpose of this initiative is to strengthen the protection of children. Technological solutions serve only as supporting tools for achieving this objective and must always remain subordinate to the protection of human rights, privacy, and the best interests of the child.

The key message of this initiative is the following:

If there is a technology capable of saving the life of a missing child, it is the duty of the State to at least examine its constitutional, legal, and technical feasibility.

19.2 Proposal for a Pilot Project

To move from the conceptual level to operational validation, the implementation of a pilot project is proposed.

Possible framework of the pilot project:

- **Scope:** 100-500 children,
- **Duration:** 12 months.

Participation:

- one hospital,
- one police unit,
- a limited number of volunteer families.

Objectives of the pilot project:

- verify the technical feasibility,
- verify legal compliance in practice,
- assess the user experience,
- verify the security mechanisms,
- identify potential risks.

The pilot project would represent a key step before any broader implementation of the system.

20. OFFICIAL PROPOSAL TO THE GOVERNMENT OF THE REPUBLIC OF SLOVENIA

We propose that the **Government of the Republic of Slovenia** examine the possibility of initiating a professional and public discussion on the establishment of a special, strictly limited, and voluntary identification system whose exclusive purpose would be the protection of children against:

- child trafficking,
- child abduction at birth,
- slavery,
- sexual exploitation,
- illegal adoptions,
- other particularly serious violations of the rights of children.

Any potential solution must be:

- strictly limited to its intended purpose,
- subject to judicial and independent oversight,

- in accordance with the **Constitution of the Republic of Slovenia**,
- in accordance with **European Union legislation**,
- technically designed to prevent misuse.

21. LEGAL ARGUMENTS FOR FURTHER PROFESSIONAL DISCUSSION

21.1 Expanded Legal Arguments

Arguments in Favour

- the protection of children as a constitutionally protected value,
- faster identification of missing children,
- strengthening legal certainty in particularly sensitive proceedings,
- prevention of organized crime,
- greater ability to verify identity in exceptional cases.

Arguments Against

- interference with the right to privacy,
- the particular sensitivity of biometric and genetic data,
- the issue of proportionality,
- the risk of security breaches or misuse,
- the risk of a future expansion of the system's intended purpose.

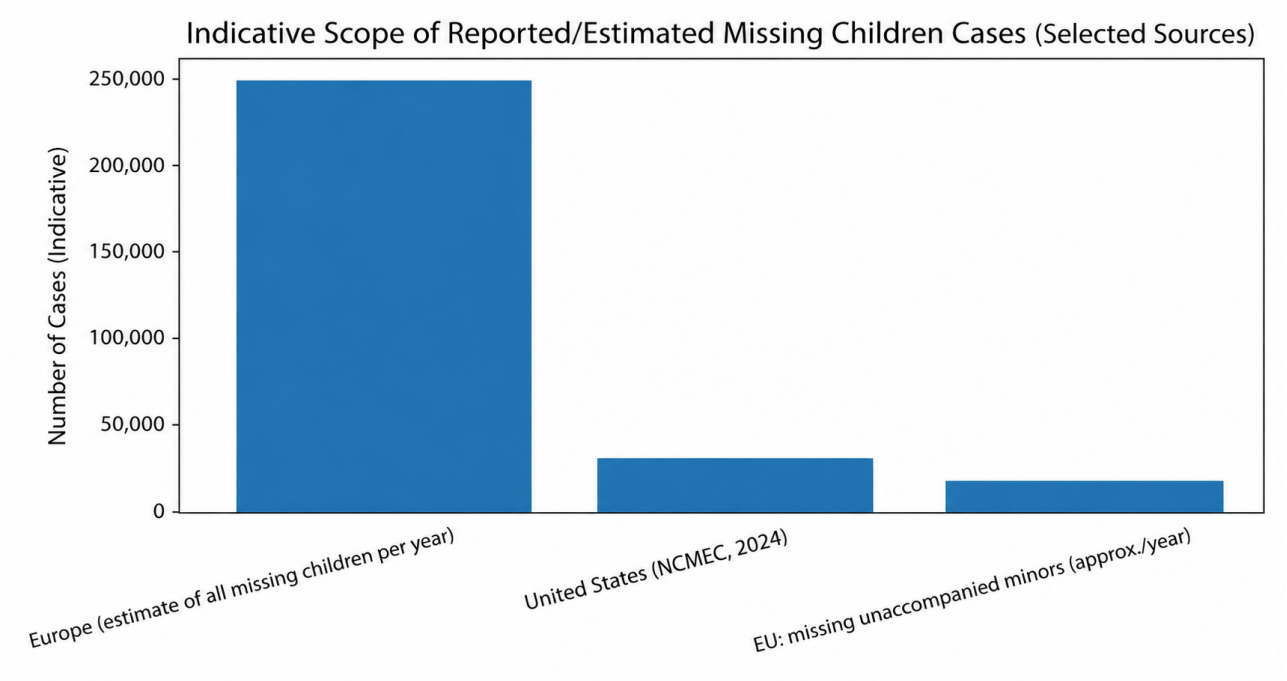
For precisely these reasons, any further discussion must be firmly grounded in law, technically verifiable, and fully transparent.

22. INDICATIVE STATISTICAL OVERVIEW AND APPENDICES

This chapter provides an overview of publicly available international data illustrating the scale of the issue of missing children, child abductions, and human trafficking. Due to differences in legal definitions, data collection methodologies, and national record systems, direct comparisons between individual countries are not always possible. The purpose of the data presented is to illustrate the approximate scale of the issue and to support a professional discussion on the need for additional protective mechanisms for children.

22.1 Indicative Statistical Overview

To provide a better understanding of the scale of the issue, selected statistical indicators from the **United States of America**, **Europe**, and the **global environment** are presented below. The overview is based on data from the **National Center for Missing & Exploited Children (NCMEC)**, the **National Crime Information Center (NCIC)**, **Missing Children Europe**, the **European Union**, and the **United Nations Office on Drugs and Crime (UNODC)**.



The data presented indicate that the issues of missing children, child abductions, and human trafficking constitute a global challenge. Although data collection methodologies differ from one country to another, all available sources confirm the need for the continued development of effective protective mechanisms for children.

Region	**Missing children**	**Abductions**	**Human trafficking / children**
USA	**NCMEC (2024):** 29,568 reports of missing children. **NCIC (2024):** 349,557 reports of missing persons.	**2,366** parental abductions by a non-custodial parent. **293** abductions by a non-family (stranger) abductor.	Approximately **1 in 7** endangered runaway cases is associated with a risk of human trafficking.
Europe	**Approximately 250,000 reports of missing children annually. 2021–2023:** at least **51,433** unaccompanied migrant children reported missing.	There are no unified EU-wide statistics; data are fragmented across individual Member States.	UNODC reports various forms of child exploitation; the proportions vary between countries.

Global	There are no unified, globally comparable statistics.	There are no unified global statistics on child abductions.	UNODC (2022): **69,627** detected victims of human trafficking; children accounted for approximately **38%** of all detected victims.

Note: The data are indicative and intended for comparative purposes. Due to differences in legal definitions and methodologies, direct comparison between countries is not always possible.

Sources: NCMEC, NCIC, Missing Children Europe, European Union, UNODC – Global Report on Trafficking in Persons.

22.2 Abductions or Unlawful Removal of Newborns from Maternity Hospitals

The abduction or unlawful removal of newborns from maternity hospitals is among the most sensitive forms of criminal offences against children. Although such cases are statistically rare in most developed countries, they are of exceptional significance because of their lasting consequences for the child, the parents, and society.

Due to non-uniform legal definitions, different reporting methods, and fragmented record systems, there is currently no single global statistic that would allow direct comparison between countries. Individual countries maintain records according to different criteria; therefore, international comparisons are limited.

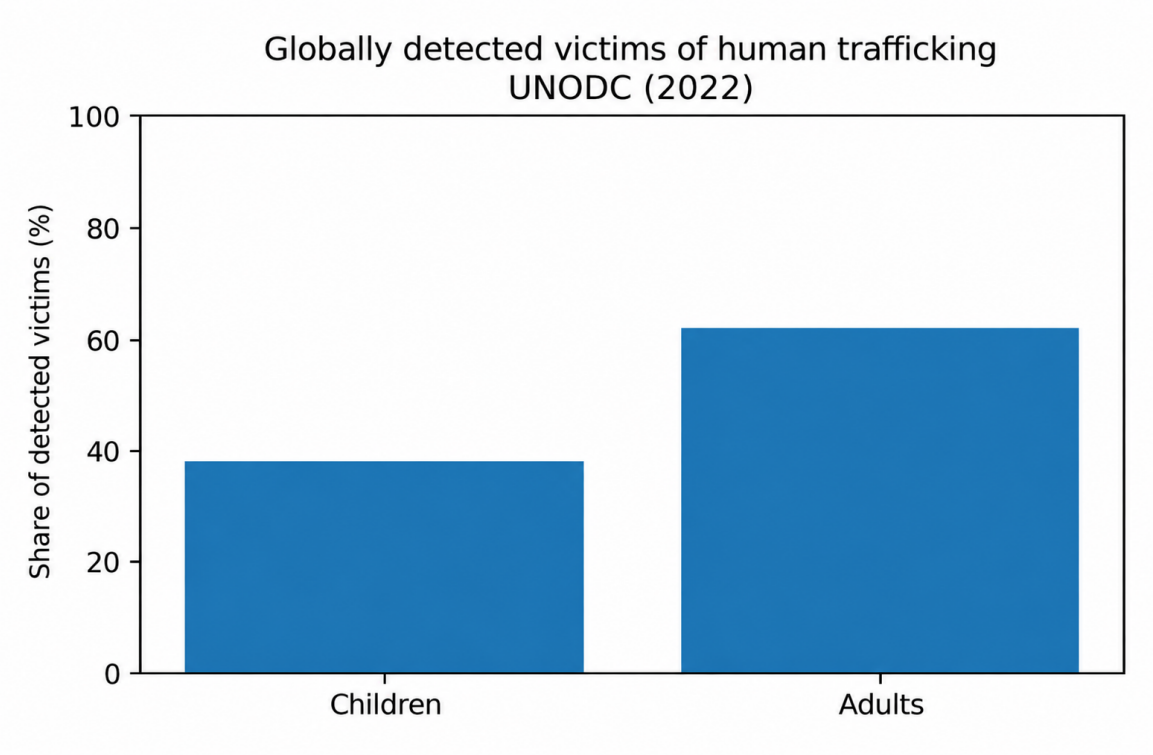
Regardless of their rarity, such cases represent one of the most serious violations of the rights of the child. For this reason, many experts emphasize the importance of preventive measures, the rapid identification of children, and effective cooperation among healthcare institutions, the police, judicial authorities, and social work centres.

The proposed **QEI** system is designed as a voluntary, strictly legally limited, and privacy-preserving protective mechanism whose purpose is not the surveillance of individuals but rather to facilitate the faster identification of children in exceptional cases of abduction, unlawful removal, or human trafficking.

Although such cases are statistically rare, their consequences for the child, the family, and society justify consideration of additional protective mechanisms that, while respecting human rights, privacy, and the principle of voluntary participation, could enable the faster identification of a child under exceptional circumstances.

22.3 Global Human Trafficking - Proportion of Child Victims

Human trafficking remains one of the most serious forms of organized crime and one of the gravest violations of human rights. Children constitute a particularly vulnerable group, as they are often victims of sexual exploitation, forced labour, forced begging, illegal adoptions, and other forms of exploitation.



According to data from the **United Nations Office on Drugs and Crime (UNODC)**, **69,627** detected victims of human trafficking were recorded worldwide in **2022**, of whom children accounted for approximately **38%** of all detected victims.

Figure: Share of children and adults among detected victims of human trafficking:

Indicator	**Value**
Recorded victims of human trafficking (2022)	**69.627**
Children	**38 %**
Adults	**62 %**

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

22.4 References for Supporting Materials / Notes

The data presented in **Chapter 22** are based on publicly available reports, official statistical records, and publications of international organizations. Due to differences in legal definitions, data collection methodologies, and national reporting systems, direct comparisons between individual countries are not always possible. The purpose of the cited sources is to provide a professional basis for discussion on child protection and to illustrate the scale of the issues addressed.

Sources used:

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. European Union

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

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

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

6. United Nations Children's Fund (UNICEF)

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

7. International Labour Organization (ILO)

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

8. International Organization for Migration (IOM)

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

Methodological Note

The numerical data used in this document provide an indicative overview of publicly available information and do not constitute a unified international statistical dataset. Differences between countries arise from differing legal definitions, national record systems, data collection methodologies, and reporting practices of the competent authorities. Consequently, direct comparisons between individual countries are not always methodologically appropriate.

The purpose of the data presented is not to provide a comprehensive statistical analysis but to illustrate the scale of the issues of missing children, child abductions, and human trafficking as a professional basis for discussion on the introduction of additional protective mechanisms.

23. CONCLUSION

This initiative is intended as a proposal for reflection, professional assessment, and public discussion regarding the possible legislative regulation of the particularly sensitive field of child protection.

The objective of this initiative is not to establish a general surveillance system, but rather to examine the possibility of developing a strictly limited, constitutionally compliant, technically secure, and legally supervised protective mechanism intended exclusively for the protection of children in the most serious and sensitive cases.

The proposed technical model is based on combining three independent biometric factors into a single cryptographic key that exists exclusively on the user's device and cannot be easily stolen, copied, or used outside the strictly defined system.

Any further consideration of such a system must be based on:

- voluntary participation,
- data minimization,
- irreversible tokenization,
- separation of records,
- judicial oversight,
- independent auditing,
- full respect for human rights.

It should further be emphasized that the proposed system is not intended to interconnect existing government records or to establish a centralized database of biometric or genetic data. The system is designed as a decentralized, user-controlled mechanism that enables identity verification exclusively in exceptional cases where existing systems do not provide reliable identification, and only on the basis of an appropriate legal basis.

Accordingly, this initiative does not constitute a proposal for the immediate implementation of a new system but rather a call for a responsible, professional, and transparent discussion on the possibilities of developing an additional protective mechanism that, while strictly respecting human rights, privacy protection, and the existing legal framework, could contribute to more effective child protection.

The final decision on any further legislative preparation or the implementation of a pilot project must be based on professional analyses, legal assessment, technical feasibility, and broad social consensus. Only in this way can it be ensured that any future solutions are effective, proportionate, constitutionally compliant, and directed toward the best interests of the child.

24. REFERENCES AND BIBLIOGRAPHY

24.1 International Legal Instruments

- Universal Declaration of Human Rights (United Nations, 1948).
- United Nations Convention on the Rights of the Child (1989).
- European Convention on Human Rights.
- Charter of Fundamental Rights of the European Union.

24.2 European Legislation

- General Data Protection Regulation (**GDPR**).
- Regulation on the European Digital Identity (**eIDAS**).
- European Union Artificial Intelligence Act (**AI Act**).

24.3 National Legislation of the Republic of Slovenia

- Constitution of the Republic of Slovenia.
- Personal Data Protection Act (**ZVOP-2**).
- Criminal Code (**KZ-1**).
- Criminal Procedure Act (**ZKP**).
- Family Code.
- Police Tasks and Powers Act (**ZNPPol**).

24.4 International Standards and Professional Guidelines

In preparing this initiative, generally recognized principles and recommendations in the following fields were also taken into account:

- information and cybersecurity,
- personal data protection,
- protection of biometric data,
- cryptographic methods,
- digital identity,
- child protection,
- prevention of human trafficking.

The recommendations and standards of international organizations were taken into consideration, including:

- International Organization for Standardization (**ISO**),
- European Union Agency for Cybersecurity (**ENISA**),
- National Institute of Standards and Technology (**NIST**),
- Europol,
- Interpol,
- UNICEF,
- Organisation for Economic Co-operation and Development (**OECD**),
- United Nations (**UN**).

24.5 Professional Literature

In preparing this initiative, generally recognized professional works in the following fields were also taken into account:

- cryptography,
- information security,
- digital identity,
- privacy protection,
- biometric systems,
- child protection and human rights.

Note

This proposed initiative is based on the legislation of the **Republic of Slovenia**, the law of the **European Union**, international conventions, and generally recognized professional principles in the fields of human rights protection, child protection, digital identity, information security, and personal data protection.

25. GLOSSARY OF KEY TERMS, ABBREVIATIONS, AND FOREIGN TERMS

To facilitate understanding of this initiative, the most important technical terms, abbreviations, and foreign expressions used in this document are explained below.

QEI (Quantized Encrypted Identity)
A cryptographically protected identification system that generates an anonymized identification token from standardized biometric templates for identity verification in strictly limited procedures.

Token
A cryptographic or technical identification record that, by itself, does not contain the direct identity of an individual.

Biometrics
The use of an individual's unique physical or behavioural characteristics (e.g., fingerprint, face, iris, or voice) to verify or confirm identity.

Biometric Template
A standardized technical representation of specific biometric characteristics that is not the same as raw biometric data.

Biometric Identification Token
An anonymized cryptographic identifier generated from standardized biometric templates that contains no personal data and does not allow the reconstruction of biometric data or the direct identification of an individual.

STR (Short Tandem Repeat)
A short repeating DNA sequence that may be used, in transformed form, as an additional biometric factor.

Cryptography
The science of protecting data through mathematical algorithms that ensure the confidentiality, integrity, and authenticity of information.

Cryptographic Key
A digital value used for encryption, authentication, or the derivation of other security keys.

Cryptographic Tokenization
The process of transforming biometric or other input data into an irreversible cryptographic record that enables the verification of a match without disclosing the original data.

Hash Function (Cryptographic Hash Function)
A mathematical function that converts input data into a unique and irreversible fixed-length output.

Irreversible Transformation
A cryptographic process in which the original data cannot be reconstructed from the generated result.

Authentication
The process of verifying that a person, device, or system is genuinely who or what it claims to be.

Multi-Factor Authentication
A method of identity verification that uses two or more independent security factors to confirm access.

Authorization
The process of determining which data or functions a user is permitted to access after successful authentication.

Audit Trail
An electronic record of all access events, verifications, and system usage that enables subsequent oversight of legality and traceability.

Separate Records
A principle according to which identity data, biometric templates, and audit records are stored in separate records, thereby significantly reducing the risk of misuse and unauthorized access.

Decentralized Architecture
An information system architecture in which sensitive data are not stored in a single central repository but are separated and protected across different security layers or records.

Decentralized Identity (DID - Decentralized Identity)
A digital identity model in which the user retains control over their identity without a central authority.

Verifiable Credentials (VC)
Digital credentials whose authenticity can be verified cryptographically.

Root of Trust
The foundation of trust within a system; the legal or technical framework that ensures the authenticity and security of the system.

Challenge-Response
A security mechanism in which the system sends a cryptographic challenge and the device returns a verifiable cryptographic response.

Threat Model
A structured analysis of potential threats, attacks, and misuse of a system.

Deepfake
Digitally generated or manipulated content created using artificial intelligence that can falsely depict an individual's face, voice, or identity.

Privacy by Design
The principle according to which privacy protection is incorporated into the design of the system from the outset.

Privacy by Default
The principle according to which the system's default settings are configured from the outset to provide the highest possible level of privacy protection.

Pseudonymization
A process in which personal data are replaced with an identifier so that an individual cannot be directly identified without additional information.

Anonymization
A process of permanently removing the possibility of identifying an individual so that the identity can no longer be determined.

Secure Enclave
A secure isolated processing module intended for the local processing of sensitive data and the secure storage of cryptographic keys.

Trusted Execution Environment (TEE)
A trusted execution environment that enables the protected execution of security-sensitive processes separately from the rest of the system.

Secure Element
A dedicated security chip designed for the protected storage of cryptographic keys and the execution of sensitive security processes.

Revocation
The process of revoking or invalidating an identification or cryptographic element.

Recovery
The process of restoring access to or recovering the system after loss, theft, or compromise.

HKDF (HMAC-based Key Derivation Function)
A cryptographic method for securely deriving new keys from existing cryptographic material.

SALT
A random value added to data before cryptographic processing to increase security and prevent predictable results.

CTX (Context)
A context linked to a specific purpose or environment that prevents the correlation of results between different systems.

Pilot Project
A limited practical trial of the system intended to verify its technical, legal, and operational feasibility.

ERAP (Emergency Response Activation Protocol)
A protocol for initiating procedures in emergency situations.

Emergency Request (ER)
A cryptographically protected request for initiating an emergency procedure within the QEI system.

PET-S (Physical Emergency Trigger Suite)
A set of physical emergency triggers that enables activation of the system without the use of biometrics.

Family Token
A cryptographic identification element intended to link members of the same family within the QEI system without disclosing their identities.

TriLock
A multi-factor security model that combines three independent biometric factors (transformed STR biometric profile, fingerprint, and facial biometrics) to generate a single cryptographic key.

QEI ONE
A proposed multifunctional security device that combines identification, cryptographic protection, and emergency procedure activation functions.

Logging
The automatic recording of all significant security events, access events, and procedures to ensure traceability and oversight.

Zero Trust
A security model in which no device or user is automatically trusted and every request is verified individually.

Fail-safe
A mode of operation in which the system enters a safe state in the event of an error and does not compromise security or privacy.

Interoperability
The ability of different systems to cooperate with one another in a technically and legally coordinated manner.

Interoperability Standard
An agreed technical standard that enables interoperability and cooperation between different information systems.

API (Application Programming Interface)
A standardized software interface that enables secure communication between different information systems.

eIDAS 2.0
The European legal framework for electronic identity, electronic identification, and trust services.

GDPR (General Data Protection Regulation)
The European Union regulation on the protection of personal data, which establishes the rules for the lawful processing of personal data.

Principle of Least Privilege
An information security principle according to which every user or system is granted only those permissions that are strictly necessary to perform its tasks.

ANNEX I - ADDITIONAL PROFESSIONAL SUPPLEMENT: MISSING KEY ELEMENTS FOR REAL-WORLD IMPLEMENTATION

I.1 Root of Trust

The current conceptual model envisages a certification or validation layer; however, for legal and systemic credibility, it must be clearly defined who actually constitutes the **Root of Trust** of the system.

The key question is whether:

- the State is the root of trust,
- it is based on a European trust framework,
- a private, but strictly regulated, entity is possible,
- the system must be linked to the **eIDAS** framework.

Without a clearly defined **Root of Trust**, it is impossible to ensure:

- the legal validity of signatures,
- institutional trust,
- mutual recognition of results,
- operational use in official procedures.

Therefore, in the next phase of professional assessment, it should be clearly established that the root of trust should be embedded within:

- the national legal framework,
- the European electronic identity framework,
- or another legally established high-assurance trust framework.

I.2 Legal Basis (GDPR + eIDAS + National Framework)

It is not sufficient for the system merely to avoid storing raw data. The law governs not only storage but also:

- processing,
- purpose,
- legal basis,
- controller,
- the rights of the individual,
- security measures,
- deletion and revocation procedures.

Therefore, every future version of the project should explicitly define:

- the legal basis under **Article 6 of the GDPR**,
- the legal basis for processing special categories of data under **Article 9 of the GDPR**,

- the relationship to the public interest,
- the relationship to explicit consent,
- the roles of the controller and the processor,
- the right to erasure,
- the right to be informed,
- the right to an audit of interventions,
- the relationship to the future **eIDAS 2.0** framework.

I.3 Key Management

One of the most important practical open issues of the system is the management of cryptographic keys and the lifecycle of identity material.

At a minimum, the following questions must be answered:

- what happens if the user loses the token,
- whether the user loses access to their identity,
- how recovery is performed,
- how revocation is carried out,
- how misuse is prevented following theft or compromise.

Therefore, the system must necessarily provide:

- a **recovery** mechanism,
- a **revocation** mechanism,
- a multi-factor recovery procedure,
- the possibility of incorporating a family-based or institutional verification model,
- time-bound and legally traceable deactivation of a compromised token.

I.4 Standards and Interoperability

At present, the system is described as a standalone conceptual framework. However, for practical deployment, it must be capable of interoperability with existing systems.

At a minimum, the following should be defined:

- the token format,
- transmission standards,
- API mechanisms,
- communication protocols,
- compatibility with government systems,
- compliance with European digital identity frameworks.

If the system is not interoperable, it remains a closed concept without practical applicability in:

- police procedures,
- cross-border cases,
- hospital environments,
- administrative procedures,
- European interoperable systems.

I.5 Verification Flow

For legal and technical credibility, it is not sufficient to describe only the token itself. The identity verification procedure must also be defined precisely.

The following must be described:

- who initiates the procedure,
- who can view the individual fragments,
- who combines them,
- who verifies the cryptographic result,
- who may initiate access to the identity record,
- under what conditions the identity may be disclosed.

This means that the next version of the document must include a precise procedural verification flow for each key usage scenario.

I.6 Attacks and Misuse

Any serious institutional or European review will, among its first questions, address threats, attacks, and potential misuse.

At a minimum, the following should be defined:

- token theft,
- device cloning,
- password or key guessing attacks,
- attacks on communications,
- social engineering,
- compromise of the certification authority,
- attacks on the user's device,
- insider misuse of the system.

Therefore, further development must be supplemented with:

- a formal **Threat Model**,
- a security architecture,
- anti-cloning mechanisms,
- an approach based on a **Secure Element** security chip,
- audit records,
- emergency system lock and recovery mechanisms.

I.7 Real-World Usage Scenarios

For operational acceptability, it is essential that the system does not remain merely an abstract concept but includes clear real-world usage scenarios.

Such scenarios should include at least:

- a case involving a missing child,
- a case involving suspected illegal adoption,
- a case involving the verification of biological parentage in legally authorized proceedings,
- a case involving a physical emergency trigger,
- a case involving court-authorized identification in a particularly sensitive situation.

Only concrete scenarios make it possible to assess:

- proportionality,
- legal admissibility,
- technical feasibility,
- operational practicality.

I.8 Funding and Governance

For any serious project, the initiative must also address the following questions:

- who finances the system,
- who operates the infrastructure,
- who bears responsibility,
- who performs oversight,
- who covers the costs of certification,
- who ensures long-term maintenance.

Without answers to these questions, no system can progress from the level of an idea to the level of actual institutional consideration.

ANNEX II - ADDITIONAL SECURITY SUPPLEMENT: THREAT MODEL, SECURITY ARCHITECTURE, AND CERTIFICATION GUIDELINES

II.1 Basic Security Premise

Every system can theoretically be attacked. However, the essential difference between systems lies in how difficult they are to attack, how much damage an attack can cause, and whether the architecture itself reduces systemic risks from the outset.

The **QEI** system can be significantly more resilient than conventional centralized models if it is properly designed because it:

- does not maintain a central database of sensitive data,
- uses fragmentation,
- employs local data transformation,
- uses cryptographic mechanisms,
- enables separate storage of different system layers.

II.2 Main Attack Surfaces

An attacker may primarily target the following layers:

- the user,
- the physical token,
- the user's device,
- communications,
- the certification or institutional layer,
- recovery and revocation procedures,
- social engineering.

The greatest real-world risks are not necessarily found in mathematical cryptography but rather in:

- human error,
- theft of the physical device,
- deception of the user,
- improper key management,
- insider misuse.

II.3 Typical Attacks and Proposed Protections

a) Token Theft

The most realistic attack scenario is the physical theft of the device or security token.

Proposed protections:

- PIN protection,
- time delay after incorrect attempts,
- immediate deactivation capability,
- Secure Element security chip,
- limited functionality without an additional factor.

b) Social Engineering

The attack is often directed at the user rather than the system.

Proposed protections:

- multi-step confirmation,
- clear user warnings,
- notifications of system use,
- user education,
- emergency lock.

c) Device Attack

An attacker may target a phone, computer, or other user device.

Proposed protections:

- Trusted Execution Environment (**TEE**),
- Secure Enclave,
- key isolation,
- prohibition of exporting sensitive material,
- signing performed exclusively within the secure module.

d) Communication Attack

Possible attacks include man-in-the-middle attacks or the interception of requests.

Proposed protections:

- end-to-end encryption,
- signed requests,
- challenge–response mechanism,
- verification of request integrity.

e) Attack on Institutions

An attack may target the certification or signing authority.

Proposed protections:

- no storage of raw biometric data,
- strict separation of functions,

- audit trail,
- multi-level oversight,
- regular security assessments.

II.4 Layered Security Architecture

The recommended system architecture should follow the principle of **defense in depth**.

Layer 1 - Device Security

- Secure Element security chip,
- anti-tamper protection,
- encrypted data storage.

Layer 2 - Crypto Layer

- biometric hashing or transformation,
- digital signatures,
- key isolation,
- HKDF or comparable key derivation mechanisms.

Layer 3 - Communication Layer

- end-to-end encryption,
- signed requests,
- integrity verification.

Layer 4 - Policy Layer

- family oversight,
- adaptive access,
- legal access rules,
- judicial or institutional activation requirements.

Layer 5 - Emergency Layer

- ERAP,
- emergency lock,
- recovery,
- revocation.

The fundamental security principle is that an attacker must compromise multiple layers of the system simultaneously rather than a single point of failure.

II.5 Certification and Standardization Guidelines

If the proposed system progresses to a formal development programme or pilot implementation, it should be aligned with internationally recognized standards and regulatory frameworks accepted by public authorities, the European Union, and institutional stakeholders.

The key reference frameworks include:

- **ISO/IEC 27001** - Information Security Management,
- **FIDO2** - Passwordless Authentication and Hardware Authentication,
- **Common Criteria EAL5+** or an equivalent assurance level - for security devices and security chips,
- **eIDAS / eIDAS 2.0** - the European Union electronic identity framework,
- compliance with the **GDPR** and national legislation.

II.6 Key Conclusion of the Security Supplement

The greatest challenge of such a system is not technology alone, but the combination of:

- legal compliance,
- certification,
- institutional trust,
- clear governance,
- demonstrable security.

The **QEI** system can represent a serious security concept only if it is designed from the outset to be:

- legally defensible,
- technically decentralized,
- operationally verifiable,
- certified,
- fully auditable.

ANNEX III - OPERATIONAL FRAMEWORK FOR THE FURTHER CONSIDERATION OF THE INITIATIVE

For the effective further consideration of this initiative, it is important to emphasize that the diagram, the basic concept, or presentation materials alone are not sufficient for institutional assessment. A structured document that can be understood and evaluated by the following is required for serious legal, professional, and administrative consideration:

- ministries,
- institutions of the European Union,
- regulatory authorities,
- legal experts,
- technology partners,
- supervisory authorities.

Accordingly, it is advisable that further work be directed toward the following operational steps.

III.1 Preparation of a Unified Formal Document

A unified, comprehensive, and internally consistent version of the initiative should be prepared, containing at least:

- the title and identification of the initiative,
- an Executive Summary,
- a clear definition of the problem,
- a description of the proposed solution,
- the legal framework,
- the technical framework,
- specific usage scenarios,
- security mechanisms,
- proposed next steps.

Such a document must be suitable for formal submission to the competent authorities and must not remain merely a conceptual presentation.

III.2 Legal Supplementation and Validation

Before the document is used in communication with institutions, it is recommended that it be further aligned from a legal perspective and explicitly define:

- the legal bases under **Article 6 of the GDPR**,
- the legal bases under **Article 9 of the GDPR**,
- the relationship between consent and the public interest,
- the roles of the controller and the processor,
- the regime governing erasure, revocation, and the rights of the individual,
- the issue of judicial oversight,
- the relationship to **eIDAS** and any future European frameworks.

Such legal validation would significantly strengthen the seriousness and credibility of the initiative.

III.3 Focusing on the Core Purpose

For institutional acceptability, it is particularly important that the initiative remains focused on its core purpose throughout all subsequent stages. The central message of the document must remain clear and understandable:

- protection of children,
- identification in exceptional and particularly sensitive cases,
- the absence of a central database,
- strict legal limitation of use,
- a high level of privacy protection.

Additional functionalities may remain as possible future extensions, but they must not obscure the fundamental objective of the initiative.

III.4 Identification of the Competent Recipients

For the further consideration of the initiative, it is important that the document be submitted to clearly identified institutions rather than to undefined or general recipients. Potential competent recipients include, in particular:

- **European Commission - Directorate-General for Justice and Consumers (DG JUST)**,
- **European Commission - Directorate-General for Migration and Home Affairs (DG HOME)**,
- **Ministry of the Interior of the Republic of Slovenia**,
- **Ministry of Justice of the Republic of Slovenia**,
- **Information Commissioner of the Republic of Slovenia**,
- **Human Rights Ombudsman of the Republic of Slovenia**,
- **the competent committees of the National Assembly of the Republic of Slovenia**,
- other competent authorities, depending on the subject matter of each phase of the initiative.

Clearly identifying the recipients contributes to greater procedural seriousness and more focused subsequent communication.

III.5 Submission of the Initiative as an Official Document

The initiative should be submitted to the competent authorities as a unified, structured, and legally and technically harmonized document.

All subsequent communication should be based on a single version of the text that clearly defines:

- the purpose of the initiative,
- the legal framework,
- the technical design,
- safeguards against misuse,
- institutional significance,
- the proposed next steps.

Such an approach is significantly more appropriate than presenting individual parts of the concept separately or repeatedly modifying them.

III.6 Final Operational Direction

The key next step is not merely the further refinement of the idea but its stabilization in the form of a document that is sufficiently clear, comprehensive, and professionally substantiated to be submitted for formal consideration.

From an operational perspective, the most appropriate course of action is therefore to:

- prepare the final harmonized version of the initiative,
- carry out basic legal and technical validation,
- identify the initial institutional recipients,
- submit the document as an official initiative for the launch of a professional and public discussion.

Such an approach provides a structured foundation for further dialogue with national authorities, the institutions of the European Union, the academic community, and other relevant stakeholders, while preserving the fundamental objectives of the initiative, its legal compliance, and its technical integrity.

INSTITUTE 1. APRIL

Research • Innovation • Advanced Technologies

REPUBLIC OF SLOVENIA
GOVERNMENT OF THE REPUBLIC OF SLOVENIA

QEI HUMANITARIAN SYSTEM FOR IDENTITY AND AID (QHIAS)

DIGITAL IDENTITY FOR ACCESS TO HUMANITARIAN AID FOR REFUGEES, MIGRANTS AND OTHER VULNERABLE GROUPS

A RESEARCH PROJECT PROPOSED FOR THE REPUBLIC OF SLOVENIA AND THE EUROPEAN UNION – FOR A SAFE, HUMANITARIAN AND DIGITAL EUROPE

QHIAS is a secure digital identity system designed to enable access to essential services, humanitarian aid and protection – without the need for storing biometric data in central databases.

KEY FEATURES:

- Secure identification without storing biometric data
- Access to humanitarian aid and essential services
- Prevention of abuse and creation of multiple identities
- Protection of unaccompanied and separated children
- Compliance with GDPR and human rights
- Monitoring and reporting for public institutions



DIGITAL WALLET

ACCESS TO FINANCIAL RESOURCES AND AID

Secure distribution of financial resources, vouchers for food, accommodation, healthcare, education and more.

HUMANITARIAN AID

FOOD, SHELTER, HEALTHCARE, AND EDUCATION

Fast and effective delivery of aid in emergencies and humanitarian situations.

PROTECTION OF UNACCOMPANIED CHILDREN

IDENTIFICATION AND BEST INTEREST PROTECTION

Special mechanism for identifying and protecting unaccompanied and separated children from their families.

PRIVACY AND SECURITY

DATA PROTECTION WITHOUT UNNECESSARY SURVEILLANCE

Strong encryption, voluntary consent and transparent management of personal data.

IDENTITY. PROTECTION. AID. DIGNITY.

HUMAN DIGNITY · PRIVACY BY DESIGN · SECURITY · TRANSPARENCY · ACCOUNTABILITY · SOLIDARITY

GDPR COMPLIANT

The project is GDPR-compliant, aligned with EU regulations and international humanitarian standards.

Proposer: Institute 1. April | Izola, Slovenia | 2026 | institut1april.com

ANNEX IV - QEI HUMANITARIAN IDENTITY AND AID SYSTEM (QHIAS)

ADDITIONAL POTENTIAL APPLICATION OF QEI TECHNOLOGY FOR THE PROTECTION OF REFUGEES, MIGRANTS, AND OTHER VULNERABLE GROUPS

IV.1 Introduction

Over recent decades, the European Union has faced increasing migration flows, humanitarian crises, wars, natural disasters, and cases of human trafficking.

Particularly vulnerable groups include:

- unaccompanied children,
- persons without identity documents,
- refugees,
- migrants,
- victims of human trafficking,
- persons who, due to wars or disasters, have lost the ability to prove their identity.

The purpose of this annex is to present the potential use of the **QHIAS (QEI Humanitarian Identity & Aid System)** as a humanitarian identity framework that could contribute to the protection of fundamental rights, facilitate secure and reliable identity verification, and support the transparent delivery of humanitarian assistance, while fully respecting the individual's right to privacy and applicable legal safeguards.

IV.2 Purpose of the System

The **QHIAS (QEI Humanitarian Identity & Aid System)** is conceived as a voluntary, privacy-oriented, and technologically advanced system designed to support humanitarian programmes.

Its objectives include:

- protection of unaccompanied children,
- protection of refugees and migrants,
- prevention of human trafficking,
- prevention of identity theft,
- reduction of abuse within humanitarian systems,
- faster identification of undocumented persons,
- more efficient access to social and healthcare services,
- more transparent management of humanitarian assistance.

IV.3 Humanitarian Digital Identity

Each eligible beneficiary could receive:

- a **QEI identification security key**,
- an **NFC identification card**,
- a **QR identifier**,
- a **digital identity**,
- a **personal security PIN**.

Identity is based on a cryptographically protected **QEI token** and does not contain raw biometric data.

The system does not establish a centralized biometric database and does not enable mass surveillance of the population.

Access to identity is possible exclusively within the framework of applicable legislation, defined procedures, and appropriate oversight.

IV.4 Humanitarian Digital Wallet

The **QHIAS** framework may include a humanitarian digital wallet designed to support the secure, transparent, and accountable delivery of humanitarian assistance.

Its use could facilitate:

- food vouchers,
- humanitarian transfers,
- social assistance,
- access to healthcare services,
- educational programmes,
- housing assistance,
- emergency assistance during crises.

Funding may be provided by:

- the European Union,
- Member States,
- international organizations,
- humanitarian organizations,
- public assistance programmes.

The system enables the traceability of public funds and reduces the potential for misuse.

IV.5 Protection of Unaccompanied Children

Particular attention is devoted to the protection of unaccompanied children, who represent one of the most vulnerable groups in humanitarian and migration contexts.

The system may assist with:

- faster identification of the child,
- protection against child trafficking,
- prevention of illegal adoptions,

- protection against exploitation,
- family reunification,
- protection of children in refugee centres.

The purpose of the proposed system is not to monitor or track children, but to strengthen their protection, safeguard their rights, and support competent authorities and humanitarian organizations in acting in the best interests of the child, in accordance with applicable legal standards and human rights principles.

IV.6 Prevention of Human Trafficking

Human trafficking remains one of the most serious threats to vulnerable individuals, particularly children, refugees, migrants, and other persons at risk of exploitation.

The proposed **QHIAS** framework may serve as a complementary protective mechanism supporting the detection and prevention of:

- human trafficking,
- sexual exploitation,
- forced labour,
- organized crime,
- illegal migration networks.

The proposed system is not intended to replace criminal investigations or judicial proceedings. Instead, it is designed to complement existing legal and institutional mechanisms by supporting secure identity verification in strictly defined, legally authorized circumstances and in full compliance with applicable laws and fundamental rights.

IV.7 Legal and Ethical Safeguards

The proposed **QHIAS** framework should be based on the following principles:

- respect for human rights,
- compliance with the GDPR,
- the principle of **Privacy by Design**,
- the principle of **Data Minimization**,
- the principle of **Purpose Limitation**,
- prohibition of discrimination,
- prohibition of political use,
- prohibition of mass surveillance,
- complete audit traceability.

The system must not enable:

- political profiling,
- religious profiling,
- tracking of an individual's location,
- commercial use of data,
- automated decision-making without human oversight.

IV.8 Smart Distribution of Humanitarian Assistance

In the future, the system could enable:

- faster distribution of assistance,
- prevention of duplicate payments,
- reduction of administrative costs,
- improved oversight of public expenditure,
- more effective assistance during natural disasters,
- more effective assistance during wars and crises.

Any future implementation of these capabilities must remain subject to applicable legal safeguards, appropriate institutional oversight, and the fundamental principles of transparency, proportionality, and the protection of fundamental rights.

IV.9 Digital Identity for Undocumented Persons

Many individuals lose their identity documents as a result of armed conflicts, natural disasters, humanitarian crises, or forced displacement.

The proposed **QHIAS** framework could support the issuance of a temporary humanitarian digital identity to facilitate access to:

- basic healthcare,
- humanitarian assistance,
- social programmes,
- education,
- legal aid.

Such a humanitarian digital identity is not intended to replace citizenship, nationality, lawful residence, or any other legally recognized civil status.

Instead, it is designed to provide a temporary and secure means of accessing essential services while the individual's legal identity or status is being established or verified in accordance with applicable national law, European Union law, and international law.

IV.10 Potential Integration with the European Digital Identity Framework

As the European digital identity ecosystem continues to evolve, interoperability between the proposed **QHIAS** framework and existing as well as future European identity infrastructures may be explored.

Potential areas of interoperability include:

- **eIDAS 2.0**,
- the **European Digital Identity Wallet (EUDI Wallet)**,
- **Decentralized Identifiers (DID)**,
- **Verifiable Credentials (VC)**.

Such integration must always respect:

- national constitutional frameworks,
- European Union legislation,
- applicable data protection and privacy laws,
- the principles of necessity, proportionality, and purpose limitation.

Any such interoperability should only be considered where it supports the humanitarian objectives of the system and does not compromise the privacy, security, or fundamental rights of the individuals concerned.

IV.11 European Union Pilot Project

To assess the feasibility and potential benefits of the proposed **QHIAS** framework within a controlled and legally compliant environment, consideration may be given to a voluntary pilot project.

Possible partners include:

- the **European Commission**,
- **UNICEF**,
- the **United Nations High Commissioner for Refugees (UNHCR)**,
- the **European Union Agency for Asylum (EUAA)**,
- the **European Border and Coast Guard Agency (Frontex)**,
- the Member States of the European Union.

The objectives of the pilot project could include:

- assessing the technical feasibility of the proposed framework,
- assessing compliance with applicable legal and regulatory requirements,
- assessing implementation and operational costs,
- assessing the potential impact on fundamental rights and data protection,
- assessing the potential benefits for the protection of vulnerable persons, particularly children, refugees, migrants, and victims of human trafficking.

Any pilot project should be conducted exclusively on a voluntary basis, under independent oversight, and in full compliance with applicable national legislation, European Union law, and international human rights standards.

IV.12 Conclusion

The **QEI Humanitarian Identity & Aid System (QHIAS)** represents a potential humanitarian application of the **QEI** framework, designed to support the protection of refugees, migrants, unaccompanied children, and other vulnerable persons.

The purpose of the proposed system is not to enable population surveillance, but rather to strengthen the protection of fundamental rights, improve the secure and transparent delivery of humanitarian assistance, contribute to the prevention of human trafficking, and provide a privacy-preserving digital identity framework for humanitarian purposes.

Any future consideration, development, or implementation of the proposed framework should be based on a comprehensive legal, technical, ethical, and operational assessment and should comply with the highest standards of human rights protection, privacy, data protection, security, and institutional accountability.

The proposed framework should be regarded as a basis for further professional discussion and evaluation rather than as a proposal for immediate implementation. Any future application should be subject to voluntary participation, democratic oversight, and full compliance with applicable national legal frameworks, European Union law, and international legal frameworks.

ANNEX V - TECHNICAL ARCHITECTURE AND FUTURE DEVELOPMENT MODEL OF THE QEI SYSTEM

ADDITIONAL PROFESSIONAL SUPPLEMENT FOR THE FUTURE DEVELOPMENT OF DIGITAL IDENTITY, CRYPTOGRAPHIC AUTHENTICATION, AND DECENTRALIZED IDENTITY SYSTEMS

V.1 Purpose of the Annex

The purpose of this annex is to present possible technical directions for the future development of the **QEI (Quantized Encrypted Identity)** framework and to outline potential implementations of an advanced digital identity architecture that combines biometrics, cryptography, decentralized identity technologies, and modern security mechanisms.

This annex does not constitute a final technical specification. Instead, it provides a framework for research and development intended to support further professional assessment, technical evaluation, pilot projects, and potential future implementation at the national, European, or international level.

V.2 Multi-Factor Biometric Model

The proposed **QEI** framework is based on the concept of combining multiple independent biometric factors to achieve a high level of reliability, security, and resilience.

Possible biometric factors include:

- fingerprint,
- facial biometrics,
- voice pattern,
- iris,
- facial geometry,
- skin markers,
- birthmarks,
- scars,
- tattoos,
- other permissible biometric characteristics,
- optionally transformed STR markers.

Each biometric factor is converted into a standardized biometric template before any cryptographic processing takes place.

The proposed framework does not use raw biometric data as an identity identifier. Instead, biometric data serve exclusively as local input for generating cryptographic material in accordance with the principles of data minimization, privacy by design, and secure identity verification.

V.3 Biometric Data Stabilization

Because biometric captures naturally vary between individual authentication attempts, the proposed **QEI** framework incorporates additional stabilization mechanisms to ensure consistent and reliable cryptographic processing.

These mechanisms may include:

- fuzzy extractor,
- error correction codes (**ECC**),
- quantization methods,
- feature normalization,
- template stabilization.

Examples:

Table: Biometric Factor and Standardized Representation

Biometric factor	**Standardized presentation**
Fingerprint	Feature Vector
Face	Embedding Vector
Voice	Voice Embedding
Tattoo	Texture Descriptor

Note: *A standardized representation is a technical representation of a biometric characteristic and is not the same as raw biometric data.*

Following the stabilization process, the system derives the corresponding cryptographic material from each biometric factor, for example:

K_FP

K_FACE

K_VOICE

K_BODY

These values represent cryptographic material derived from standardized biometric templates rather than from the biometric data themselves.

This approach enables the system to produce the same, or a sufficiently consistent, cryptographic result from naturally varying biometric captures for subsequent use. In doing so, it ensures reliable authentication while maintaining a high level of privacy and security for biometric information.

V.4 Generation of the Cryptographic Identity

The final cryptographic identity key is generated by combining multiple independent biometric and security factors.

Example:

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

Where:

- **K_FP** = cryptographic material derived from the fingerprint,
- **K_FACE** = cryptographic material derived from facial biometrics,
- **K_BODY** = cryptographic material derived from physical markers, such as birthmarks, scars, or tattoos,
- **SALT** = a random security parameter that ensures uniqueness and resistance to precomputed attacks,
- **CTX (Context)** = the context of use, linked to a specific purpose or environment, preventing the correlation of results between different systems or use cases.

This approach ensures that the final cryptographic key is not dependent on a single biometric factor but instead represents the result of a secure combination of multiple independent inputs together with additional cryptographic security elements.

From the resulting key, the following is generated:

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

The **QEI token**:

- does not contain personal data,
- does not contain biometric data,
- does not allow the reconstruction of identity,
- does not allow the reconstruction of biometric data,
- does not contain health or genetic information.

The **QEI token** serves exclusively as an anonymized cryptographic identifier and is intended solely for identity verification within legally authorized and strictly supervised procedures. By itself, it neither discloses nor represents the identity of an individual.

V.5 Local Processing and Secure Modules

All biometric data are processed exclusively locally.

Supported environments may include:

- **Trusted Execution Environment (TEE)**,
- **Secure Enclave**,
- **Secure Element**,
- **StrongBox**,
- **Hardware Security Module (HSM)**,
- other certified security modules.

Biometric data never leave the device in raw or reconstructable form.

The server receives only:

- the **QEI token**,
- the public key,
- cryptographically signed results.

This architecture significantly reduces the risk of biometric data theft, large-scale data breaches, and unauthorized mass exploitation by ensuring that sensitive biometric data remain confined to trusted local processing environments.

V.6 Cryptographic Authentication

The system uses a **Challenge-Response** mechanism.

Procedure:

- the server sends a cryptographic challenge,
- the device locally generates or unlocks **K_FINAL**,
- the device creates a digital signature,
- the server verifies the signature.

The system never transmits:

- raw biometric data,
- biometric templates,
- genetic data,
- personal data.

The outcome is:

- access granted,
- access denied,
- additional factor required.

This architecture provides a high level of privacy and security.

V.7 Decentralized Digital Identity

The **QEI** framework is designed to support interoperability with decentralized digital identity ecosystems and modern standards for identity verification and the exchange of digital credentials.

Illustrative conceptual flow:

Biometrics

↓

QEI

↓

Ed25519 Key Pair

↓

W3C DID Digital Identity

Potential interoperability includes:

- **W3C DID** (Decentralized Identifiers),
- **Verifiable Credentials (VC)**,
- **Hyperledger Foundation**,
- digital identity projects of the **Linux Foundation**,
- **eIDAS 2.0**,
- the **European Digital Identity Wallet (EUDI Wallet)**.

This approach enables the establishment of a digital identity without relying on passwords, physical identity documents, or centralized databases.

The individual remains the primary controller of their digital identity and retains control over the use and disclosure of their digital credentials in accordance with applicable legislation and privacy principles.

V.8 Potential Products and Areas of Application

Based on the **QEI** system, a variety of different solutions can be developed.

QEI Card

A smart card with an integrated security element.

Possible applications:

- electronic identity,
- healthcare systems,
- public administration,
- banking.

QEI Mobile Application

A mobile application providing passwordless digital identity.

Example of use:

Facial recognition + fingerprint = digital identity

QEI Border System

An advanced identification system for border crossings.

QEI Humanitarian System

A digital identity solution for refugees, migrants, and humanitarian programmes.

QEI Child Protection System

Protection of children, missing persons, and the prevention of human trafficking.

QEI Secure Vault

Protection of:

- digital assets,
- cryptocurrency wallets,
- sensitive documents,
- trade secrets.

QEI Citizen System

A future digital identity solution for citizens.

QEI Healthcare System

A secure identity solution for healthcare systems and medical records.

V.9 Identity Lifecycle Management

One of the key advantages of the **QEI** framework is its ability to regenerate cryptographic identity material without requiring any change to an individual's biological characteristics.

Procedure:

- generate a new **SALT**,
- define a new **CTX**,
- perform a new cryptographic transformation,
- generate a new **QEI token**,
- deactivate the previous identity material.

This approach enables the framework to restore security after the loss, theft, or compromise of identity-related cryptographic material without requiring new biometric characteristics.

Compared with conventional biometric identification systems, this capability provides a significant security advantage by supporting secure identity recovery while preserving the individual's existing biometric characteristics.

V.10 Security Advantages of the Architecture

The proposed **QEI** architecture combines several complementary security mechanisms, including:

- multi-factor biometrics,
- local processing,
- cryptographic tokenization,
- decentralized identities,
- revocation and regeneration capabilities,
- the absence of a centralized biometric database,
- a high level of privacy.

The architecture is designed in accordance with the following internationally recognized security and privacy principles:

- **Privacy by Design** - privacy protection built into the system by design,
- **Privacy by Default** - privacy protection as the default configuration,
- **Data Minimization** - the principle of minimizing the amount of data processed,
- **Purpose Limitation** - the principle of limiting data processing to its intended purpose,
- **Security by Design** - security incorporated into the system by design,
- **Zero Trust Principles** - principles of Zero Trust architecture.

This architectural model reduces the risks associated with centralized data repositories, strengthens resilience against cyberattacks, and enhances the protection of personal and biometric data through decentralized processing and cryptographic safeguards.

V.11 Research and Development Potential

The proposed **QEI** framework has the potential for further research and development across a broad range of application areas, including:

- digital identity,
- child protection,
- humanitarian programmes,
- public administration,
- healthcare,
- banking,
- critical infrastructure,
- cybersecurity,
- decentralized identities,
- digital wallets,
- future European identity systems.

Possible research directions include:

- artificial intelligence for identity verification,
- post-quantum cryptography,

- European digital wallets,
- interoperability between countries,
- protection of critical infrastructure,
- secure identities for the Internet of Things (**IoT**).

The proposed framework could be further developed through European research, innovation, and digital transformation programmes, including joint initiatives involving public authorities, research institutions, universities, industrial partners, and the institutions of the European Union.

V.12 Conclusion

The key innovation of the **QEI** system is not an individual biometric factor but the combination of:

- multiple independent biometric factors,
- **Fuzzy Extractor** technology,
- local processing within a **Trusted Execution Environment (TEE)** or an equivalent secure execution environment,
- cryptographic tokenization,
- identity regeneration using **SALT** and **CTX** parameters,
- decentralized digital identities,
- modern cryptographic mechanisms.

Such an architecture represents a potential foundation for future generations of digital identities that combine a high level of security, privacy, interoperability, and usability, and that may contribute to the development of a safer digital society within the European Union and beyond.



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

QEI INITIATIVE

FOR A SAFER, FAIRER AND MORE HUMAN-CENTERED FUTURE



OUR VISION

To create a world in which every individual is safely recognized, protected and treated with dignity – regardless of age, nationality, origin or circumstances.

OUR MISSION

Through the innovative Quantized Encrypted Identity (QEI) system, we support the protection of children, refugees, migrants and all vulnerable groups and contribute to combating human trafficking, respecting human rights and making humanitarian aid more effective worldwide.

OUR VALUES

- Respect for human rights and human dignity
- Data privacy and protection
- Anonymization and data minimization
- Transparency and legal compliance
- Innovation and technological excellence
- Solidarity and humanity

QEI – THE IDENTITY OF THE FUTURE

FOR PEOPLE. FOR SOCIETY. FOR THE WORLD.

CHILD PROTECTION

Protection of unaccompanied children, missing children and prevention of child trafficking.

REFUGEES AND MIGRANTS

Secure identity and access to services for refugees, migrants and other vulnerable groups.

HUMANITARIAN AID

Effective, secured and traceable distribution of aid in humanitarian situations.

PRIVACY AND SECURITY

Cryptographic protection, local storage and no storage of raw biometric data.

GLOBAL IMPACT

Aligned with European standards (eIDAS 2.0, GDPR) and enabling global interoperability.

TOGETHER, WE BUILD A WORLD WHERE IDENTITY IS A RIGHT, NOT A PRIVILEGE.

Aligned with European values and legal frameworks within the European Union.

Technology that puts people at the center of every solution.

Partnership for a better and safer future for all.

Institute 1.april™

RESEARCH • INNOVATION • ADVANCED TECHNOLOGIES

IDENTITY IS TRUST. TRUST IS THE FOUNDATION OF THE FUTURE.