The ECTLC-Horcrux Protocol for Decentralized Biometric-Based Self-Sovereign Identity with Time-Lapse Encryption

N. M. Kaziyeva[1], R. M. Ospanov[2], N. Issayev[3], K. Maulenov[4], Shakhmaran Seilov[5]
Faculty of Information Technology, Eurasian National University, Astana, Kazakhstan[1, 2, 3, 5]
AKHMET BAITURSYNULY Kostanay Regional University, Kostanay Kazakhstan[4]

Abstract—**In the era of rapid development of digital communication, there is a growing need for technologies that guarantee secure user identification, document authentication and protection of personal data, including biometrics. Previously used centralized identity management systems are becoming increasingly vulnerable to hacking, falsification and misuse. This problem is especially relevant when information must remain closed until a specific moment or event occurs, for example, in the fields of forensics, healthcare or law (medical certificates, legal acts, inheritance agreements, etc.). The main goal is to create a secure, verifiable and at the same time distributed access control system with the ability to defer disclosure of information. The study proposes a cryptographic protocol that combines Self-Sovereign Identity (SSI), Time-Lapse Cryptography (TLC), and decentralized biometric data management. The protocol is based on the principles of Time-Lapse Cryptography (TLC) and the Horcrux protocol, which enable time-controlled disclosure of encrypted information associated with a user's identity. The architecture includes the use of QR codes as a transport for Verifiable Credentials (VC), blockchain for authenticity verification and key management, and biometrics as a second factor of identity binding. The proposed solution is intended for use in scenarios where cryptographic protection against premature access to sensitive data is required, such as in medicine, forensics, notarial acts, or intellectual property. The study presents the protocol structure and application options.**

Keywords—Self-sovereign identity; horcrux protocol; elliptic curves time-lapse cryptography; biometrics; QR codes; blockchain

I. Introduction

With the rapid growth of digital interactions, technologies that ensure reliable identification of individuals, document authentication, and protection of sensitive personal data, including biometric information, are becoming increasingly important. Traditional centralized identity management systems are increasingly vulnerable to compromise, counterfeiting, and unauthorized access. This is especially critical in cases where data cannot be disclosed before a certain event or time, such as in forensic, medical, or legal practice (medical reports, legal documents, testaments, etc.). The main challenge is to ensure secure, verifiable, and at the same time decentralized access management with the ability to delay disclosure of information.

One promising concept that can provide a balance between reliable authentication and privacy protection is the Self-Sovereign Identity (SSI) model. It is based on the idea that a user should have full ownership of their digital identities and control over the process of their provision without the participation of centralized certifying parties. SSI uses decentralized identifiers (DIDs), cryptographically protected identities (Verifiable Credentials, VC) and blockchain as a trusted, immutable infrastructure [1-3]. However, in its basic form, SSI does not solve the problem of temporary access control and secure management of biometric information.

This work is aimed at developing a new cryptographic protocol that expands the capabilities of SSI technology by combining QR codes as a transport mechanism for distributing links to VCs and DIDs, biometrics as a factor in linking credentials to a physical identity, time-lapse encryption as a mechanism for delayed access to sensitive data, and blockchain as a decentralized platform for trust and automatic key management. The key components of the proposed solution are the Horcrux protocol [4] and the Elliptic Curves Time-Lapse Cryptography (ECTLC) protocol [5]. The Horcrux protocol is a protocol which implements cryptographic separation and multi-party management of biometric templates. It eliminates the need for centralized storage of biometrics and allows the user to safely participate in the authentication process by restoring the template only with the participation of trusted parties. The Elliptic Curves Time-Lapse Cryptography (ECTLC) protocol is a cryptographic mechanism that allows data to be encrypted with the impossibility of decrypting it before a specified time, without dependence on a trusted time server. In this study, ECTLC is used to create secure VCs with delayed activity. In addition, the architecture takes into account compatibility with the Biometric Open Protocol Standard (BOPS) [6], which defines a secure way to collect, store and transmit biometric data. Together, these mechanisms are combined into a single protocol that implements biometric SSI verification with time-based access restriction, which allows for scenarios with cryptographically secured delayed disclosure of information.

The proposed solution allows for the implementation of application scenarios in which access to credentials and sensitive data is possible only after a certain point of time. It is applicable in medicine, law, education, intellectual property and other areas where strict compliance with deadlines and provable protection of identity and data is required (e.g., delayed disclosure of wills and court documents; restriction of access to biometric data activated only by a legal or time-based software trigger; time capsules and future statements confirmed by VC and DID). Thus, such a solution makes it possible to form the basis for building trusted digital ecosystems in which the user receives technological means for managing not only identity, but also the time of access to their data, including biometrics, taking into account modern standards and decentralized protocols.

In general, the approach under consideration for the integration of SSI, TLC, QR codes, blockchain and biometrics technologies is due to the need to increase the level of trust in digital transactions, minimize the risks of personal data leakage and form identification systems that are resistant to external influences. Modern trends in the digitalization of various spheres of society (public administration, medicine, the financial sector, education, etc.) demonstrate the limitations of traditional centralized authentication mechanisms based on logins, passwords or unified registries. These models are characterized by a high degree of vulnerability to cyberattacks, leaks and misuse of information. In contrast, the concept of self-sovereign identification assumes decentralized management of personal attributes, in which the subject retains control over their own digital data and selectively discloses it depending on the context of interaction.

Using an encryption mechanism for a specified time allows expanding the functionality of identification systems, providing access to encrypted information strictly at a predetermined moment. Even if encrypted data is compromised, temporary blocking ensures that early access is impossible.

The use of QR codes provides a universal and technologically accessible channel for transmitting encrypted tokens, keys or digital certificates. This tool facilitates the coupling of physical and digital processes, allowing for the implementation of identity verification scenarios in offline environments with an instant transition to secure online interaction.

The use of biometric methods strengthens the trust basis of the system, as they allow for reliable verification that the presented digital identity actually belongs to a physical carrier. Unlike traditional authentication factors that are subject to transfer or theft, biometric features have a high degree of uniqueness and stability, which reduces the likelihood of subject substitution.

Blockchain technology guarantees the integrity and verifiability of data. This eliminates the possibility of falsifying transactions or making retroactive changes to records. The distributed structure of the registry eliminates the dependence on a centralized verification authority and eliminates the possibility of system failure. In addition, the use of smart contracts allows for automatic management of access to time-dependent resources, complementing cryptographic methods with the functionality of predefined rule execution.

As a result, SSI ensures decentralization and user control, biometrics confirm the authenticity of the individual, QR codes create a convenient interaction interface, encryption for a specified time regulates the moment of access to data, blockchain guarantees the immutability of records and automation of rules. The result is a multi-level system that combines convenience for the end user and a high level of cryptographic protection. The prospects for such integration are most significant in contexts that require a combination of confidentiality, time synchronization, and reliable identity verification.

It can be said that there are currently no works that consider the implementation of all the above components in one formal protocol at the same time. More common are works that cover two to three elements and architectural compositions that can be combined (see Table I).

TABLE I COMPARATIVE TABLE OF THE WORKS DEVOTED TO INTEGRATION OF SSI, TLC, QR CODES, BLOCKCHAIN AND BIOMETRICS TECHNOLOGIES. NOTATION: + CONSIDERED, - NOT CONSIDERED

Sources	SSI	Blockchain	Biometrics	QR-codes	TLC
[4]	+	+	+		
[7]	+	+			
[8]	+		+		
[9]	+	+	+		
[10]	+	+	+	+	
[11]	+			+	
This study	+	+	+	+	+

A. Motivation and Problem Statement

SSI improves user control and verifiability but does not guarantee cryptographic non-access to sensitive attributes before a policy time (T). Biometric authentication often relies on centralized custody. We address both gaps by combining decentralized biometric sharding with time-lapse encryption anchored to SSI.

B. Main Contributions

SSI-native protocol that binds VCs to a user via Horcrux-style biometric splitting without centralized template storage;

ECC time-lapse layer that withholds decryption capability until time (T);

Verifier workflow via QR-encoded handles to DIDs/VCs for offline/online use;

Security and deployability discussion (threat model, failure modes, regulatory aspects).

The rest of the study is organized as follows: Section II reviews IEEE Biometric Open Protocol Standard (BOPS), Self-sovereign identity technology, the Horcrux protocol and the Elliptic Curves Time-Lapse Cryptography (ECTLC) protocol. Section III presents our new cryptographic protocol for decentralized biometric-based self-sovereign identity with time-lapse encryption called the ECTLC-Horcrux protocol and considers possible use cases. Section IV presents the results. Section V details the discussion. Finally, Section VI summarizes the study.

II. RELATED WORKS AND POSITIONING

1) SSI and verifiable credentials: Surveys and standards (including W3C Verifiable Credentials v2.0 and DID Core) systematize identifiers, credential models, and wallet architectures, highlighting selective disclosure and revocation challenges. We adopt this stack to enable issuer-agnostic verification and offline validity checks [28, 29, 30].

2) Decentralized biometrics: Horcrux proposes cryptographic splitting of biometric templates to remove single points of failure. Our design reuses the splitting intuition but couples it with SSI wallets and time-based access control.

3) Time-lapse / Time-lock cryptography: ECC-based time-lapse cryptography enforces decryption only after (T) by threshold key release. We instantiate an ECC-based service and align its trust assumptions with SSI verifiers.

4) Biometric protection standards: ISO/IEC 24745:2022 provides guidance on biometric information protection; we comply by avoiding long-term template custody at the verifier and enforcing secure transport [31].

5) Positioning: Unlike prior work treating these threads separately, ECTLC-Horcrux composes SSI, decentralized biometrics, and ECC-based time-lapse into a single protocol with QR-mediated verifier flows and explicit threat considerations.

III. Methods

The protocol designed in this work is based on 2410-2017 - IEEE Biometrics Open Protocol Standard (BOPS), Self-Sovereign Identity technology, the Horcrux protocol, the Elliptic Curves Time-Lapse Cryptography (ECTLC) protocol, and the use of QR codes.

A. Biometrics Open Protocol Standard (BOPS) [6]

2410-2017 - IEEE Biometrics Open Protocol Standard (BOPS) is an open protocol designed to provide secure and trusted biometric authentication that meets the high requirements of national and international standards. The protocol covers the full cycle of working with biometric data - from their collection and storage to transmission and comparison, while implementing a multi-level security architecture.

At the Collection stage, BOPS defines the use of standard APIs for obtaining biometric templates (e.g., fingerprints, face, voice) using hardware trusted environments such as HSM (Hardware Security Module), TEE (Trusted Execution Environment) or TPM (Trusted Platform Module). The use of these modules ensures that data is collected and stored in isolated, inaccessible or encrypted memory, which significantly reduces the risk of leakage or unauthorized access.

For storage (Storage) of templates, BOPS provides for the use of secure formats and cryptographic containers with hardware encryption support. Moreover, the standard supports the cryptographic sharding mechanism, in which the biometric template is divided into several parts. One of them is stored locally on the device, and the second is either also stored locally or transmitted to a remote platform. In this case, the compromise of one of the parts does not allow the restoration of the original biometric template, which ensures resistance to leaks.

Transmission in BOPS is implemented via the Representational State Transfer (REST) interface protocol, and no biometric template can be transmitted in unencrypted form. Before sending, the data is wrapped in a cryptographic container encrypted using the server's public key generated at the registration stage. Transmission is carried out exclusively through a two-way secure TLS channel, and the client TLS certificate is installed on the mobile device in advance, at the time of installing the application.

At the Processing stage, the protocol prohibits long-term storage of templates. All matching operations are performed exclusively in RAM or in a local HSM, without using file systems, databases or other forms of persistent storage. This significantly reduces the risk of data compromise in the event of a system breach.

The BOPS protocol includes two key phases of operation: registration and authentication. In the registration phase, the server generates a key pair (RKP) by transmitting a public key to the device. On the client side, a local key pair (LKP) is generated, and the collected biometric template (initial biometric vector - IBV) is associated with this pair. The template and keys are then encrypted using RKP and transmitted to the server over a secure channel.

In the authentication phase, the protocol provides for three configurations:

1) Local match: a candidate biometric template (CBV) is collected on the device, which is matched with a reconstructed IBV collected from local and, if necessary, remote shares. The result of the match (a Boolean or numeric threshold) is encrypted and sent to the server. This configuration complies with FIDO UAF requirements, provided that a certified local authenticator is used.

2) Remote match: The CBV is encrypted and sent to the server, where it is matched against the corresponding portions of the IBV available to the server and sent from the client.

3) Combined authentication: The server can, upon request, encrypt its portions of the IBV and send them back to the client, where the match occurs. Once the match is complete, all biometric data and keys are destroyed from RAM.

To protect against man-in-the-middle (MITM) and replay attacks, BOPS uses one-time passwords and server challenges wrapped in encrypted crypto containers (envelopes), ensuring the integrity and authenticity of the transmitted data. Compared to other protocols such as FIDO UAF, BOPS offers comparable levels of security but has additional capabilities, such as remote storage, flexible sharding, and multi-level authentication, making it a more versatile solution for a variety of scenarios, including mobile platforms, cloud services, and IoT devices. However, the choice of storage and mapping mode may depend on regulatory constraints, institutional policies, and trust level requirements.

B. Self-Sovereign Identity [1-3]

Self-Sovereign Identity (SSI) is a conceptual and technical approach that gives users full control over their digital identity without dependence on centralized certifying authorities. Traditional identity models based on third-party identity providers (such as governments, banks, and commercial platforms) come with risks of compromise, centralized control, and privacy breaches. SSI addresses these shortcomings by transferring control over identity directly to the user, while ensuring verifiability and trust based on cryptographic principles. SSI is based on a model in which identifiers and their verifiable credentials are stored by the identity subject (the user) and can be provided on request to various verifiers.

The key components of the technology are the following elements:

Decentralized identifiers (DIDs) are unique, persistent identifiers that do not depend on central registries. They are managed by the user and allow the creation of cryptographically verifiable links between entities [29]. A DID is associated with a DID document containing public keys, authentication methods, and service endpoints that allow other entities to interact with the owner of the identifier.

Verifiable Credentials (VC) are digital assertions signed by an issuer (e.g., an educational institution, government agency, or employer) that a user can present to a verifier [28, 30]. Verification is performed without a request to the issuer, solely by checking the digital signature and metadata of the credential.

A digital identity wallet is a software solution (mobile or desktop) designed to securely store DIDs, private keys, and received credentials. The wallet provides an interface for interaction with issuers and verifiers, implements the functions of consent to data transfer and supports exchange protocols.

To ensure confidentiality, authenticity, and other security properties, cryptographic methods are used, including asymmetric encryption and digital signatures based on public key cryptography to ensure the authenticity of credentials; zero-knowledge proofs to confirm certain attributes (e.g. age, affiliation with an organization) without disclosing additional data.

Decentralized ledgers (ledger-based DID methods) are used to publish and resolve DIDs. Depending on the architecture, implementations based on blockchain platforms (e.g. Hyperledger Indy, Ethereum, Sovrin) or lighter methods such as DID:Web are possible. Cost efficiency is achieved through Layer-2 solutions, notably the Polygon Amoy testnet for DID anchoring. This reduces on-chain operations to ~0.002 USD per transaction while maintaining SSI revocation capabilities [27]. The implementation of the technology is provided by the W3C consortium standards, including DID Core and Verifiable Credentials Data Model.

The SSI architecture is built on a three-party interaction model, including the following roles: Issuer (an organization that creates and signs digital certificates), Holder (an entity that manages its digital identity, stores credentials in a wallet, and provides them upon request), Verifier (a party that requests and verifies the authenticity of the information received). The interaction between the parties is implemented through the exchange of verifiable credentials (Verifiable Credentials) and decentralized identifiers (DIDs).

1) The Issuer creates and signs a certificate (VC) containing a statement (e.g., "The user graduated from University N"), as well as its DID.

2) The User (Holder) receives this certificate and stores it in its digital wallet associated with its own DID and keys.

3) If necessary, the User presents the certificate to the Verifier, providing proof (possibly with zero knowledge), after which the Verifier verifies the VC signature, receives the Issuer's public key through the DID ledger, and decides on the authenticity of the presented certificate.

This three-party protocol is built without constant dependence between the participants, which allows for offline validation and increased resistance to censorship or denial of service.

C. The Horcrux Protocol [4]

The Horcrux protocol is a secure and decentralized biometric identification method within the Self-Sovereign Identity (SSI) concept. It combines the advantages of biometric methods, the 2410-2017 - IEEE Biometric Open Protocol Standard (BOPS), and the decentralized identifier (DID) infrastructure. The main idea of the protocol is to separate and decentralize the storage of user biometric data with subsequent authentication through their joint processing. This eliminates the need for centralized storage, reducing the risk of leakage and providing the user with full control over their biometric templates. The Horcrux protocol is based on dividing the user's biometric template into two encrypted parts (shares) using visual cryptography techniques. One part is stored locally on the user's device, and the other is stored in a decentralized storage associated with the DID document. This ensures the absence of a single point of failure and increases resistance to data compromise.

The protocol consists of two parts: enrollment and authentication. The enrollment process includes the following components. First, there is the collection of biometric data. The user provides biometric data (e.g. fingerprint or face image), which is converted into an initial biometric vector (IBV). Next comes splitting and encryption. The IBV is split into two shares, each of which is encrypted. One part is stored on the user's device, the other in a DID document placed in a decentralized storage (e.g. IPFS, Dropbox, Google Drive). Then a DID is created. A unique decentralized identifier (DID) is generated, which refers to the corresponding DID document containing the encrypted part of the biometric data. Finally, there is the registration in the blockchain. The DID and its corresponding DID document are registered in the blockchain, ensuring the immutability and verifiability of the data.

The authentication process consists of the following components. First, there is the collection of current biometric data. The user provides biometric data, which is converted into a candidate biometric vector (CBV). Shares extraction and merging are then performed. The local share of the IBV is combined with the share extracted from the DID document, and then compared with the CBV to verify the identity. Finally, authentication is performed. If the combined IBV matches the CBV, authentication is considered successful.

D. The Elliptic Curves Time-Lapse Cryptography (ECTLC) Protocol [5]

The Elliptic Curves Time-Lapse Cryptography (ECTLC) protocol is based on the Time-Lapse Cryptography (TLC) protocol [12]-[14], the protocol for encrypting client data in such a way as to ensure that decryption cannot occur before a certain designated time, regardless of whether the sender wishes it. TLC protocol includes Pedersen's distributed key generation protocol [15], Feldman's threshold verifiable secret sharing protocol [16], and ElGamal encryption [17]. The TLC protocol uses the agreed-upon parameters of the ElGamal encryption algorithm, including the prime number p, the generator g of prime order q. These parameters can be found, for example, in RFC 3526 [18] and RFC 5114 [19]. The ECTLC protocol uses similar elliptic curve cryptography algorithms, namely the distributed key generation protocol based on discrete logarithm on elliptic curves [20], the Pedersen verifiable threshold secret sharing protocol [21], and the ElGamal elliptic curve encryption algorithm [22], respectively. The protocol is also implemented using a Service (Time-Lapse Cryptography Service) consisting of n participants P_1, ..., P_n. Each participant of the Service P_i can be represented as an autonomous computer (server) that accurately and secretly performs the calculations required by the protocol, securely stores all its secret data, and has a secure way of backing up the data for emergency recovery. All participants of the Service can privately and secretly exchange information with each other, forming a network. A threshold value t is assumed such that at most t – 1 participants can violate the protocol, and at least t participants are reliable. The condition $n \geq 2t - 1$ ($t \leq (n+1)/2$) must be satisfied, e.g., if n = 3, then $t \leq 2$.) For further efficiency, reliability, and resistance to attacks, a small network M of K managers is used, which acts as a “control team” for the Service. This control team must create a schedule of public and corresponding private keys generated by the Service; maintain an internal bulletin board for use by Service participants; maintain an open bulletin board for Service users. The integrity of these bulletin boards is ensured by each manager maintaining their own copies of the two bulletin boards. Service participants and users will look at messages posted on each copy of the bulletin boards and determine the correct values by the majority of entries. Each Service participant digitally signs each message. The Service may generate key structures on a periodic basis; for example, it may create keys with a lifetime of 1 week every day, or create keys with a lifetime of 2 hours every 30 minutes. Such a schedule is posted by managers on an open bulletin board. In addition, the Service may accept requests from users to generate new keys with a specified lifetime; managers accept these requests and post them on an open bulletin board. Service participants create keys according to the protocol, sign them, and publish the signed key structures on an open bulletin board. The actions of all protocol participants are synchronized using publicly available and reliable clocks such as those provided by NIST. The protocol provides for the use of agreed parameters of the elliptic curve used: the modulus of the elliptic curve, a prime number p, the equation of the elliptic curve, the coefficients of the equation a and b from the field Fp, and a point of the elliptic curve G of prime order q. These parameters can be found, for example, on the SafeCurves project website [23].

E. QR Codes [24-25]

Two-dimensional matrix barcode technology, QR (Quick Response), is a means of presenting, transmitting and verifying structured digital data. Due to their compactness, high encoding density, resistance to damage and widespread support in software and hardware, QR codes are widely used in modern information systems to ensure contactless and offline transactional transfer of information. A QR code is a two-dimensional image consisting of black and white modules (squares) located in a square grid. It encodes binary or symbolic information that can be read by an optical scanner (including mobile device cameras) and converted back into the original data. Modern QR codes allow you to encode up to several thousand characters in a single image, including text, JSON structures, URLs, digital signatures and other formats. QR codes can be used to transmit structured data (e.g. JSON representation of digital certificates, access tokens, session keys, etc.), user identification (generation of personalized codes containing DID or hash identifiers for authentication), offline interaction (enabling the exchange of information between entities without a network connection), data signing and verification (inclusion of digital signatures in encoded data to ensure its authenticity when scanned), generation of passes, tickets, vouchers and transaction messages (visualization of one-time or permanent digital passes with the possibility of machine verification).

F. Biometric Data Protection Via Steganography

To ensure secure transmission of SSI credentials within TLC frameworks, QR-encoded Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs) are embedded into facial images using LSB steganography. Each credential layer is distributed across a dedicated RGB channel (e.g., VC in R, DID in G), enabling standard QR decoders to extract payloads while maintaining visual fidelity (distortion <0.1%, as validated in prior research [26]). Steganography is used only as a transport/masking channel for payloads and does not affect the cryptographic access policy; it is orthogonal to TLC/SSI and therefore optional

IV. Results

The ECTLC-Horcrux protocol describes the interaction of the following participants: the User (Holder), the ECTLC-Service, the Service Provider (Issuer), the Service Provider (Verifier), the BOPS Server A, the BOPS Server B, the Blockchain, and the Identity hub. The protocol consists of two stages: enrollment and authentication.

Step-by-step description of the protocol.

A. Enrollment

1) The User produces his biometric template (initial biometric vector) using his mobile device.

2) The produced initial biometric vector is encrypted into two shares via visual cryptography by the mobile device.

3) One share is secured on the mobile device; the second share is encrypted with the device's private key.

4) The encrypted share, the corresponding device's public key and a time value T before which access to biometric data cannot be granted are sent to the Issuer.

5) The Issuer requests the ECTLC-Service for the ECTLC-Service's public key, indicating the time value T.

6) Upon receiving the request, the ECTLC-Service generates a public key according to the ECTLC cryptographic protocol and transmits it to the Issuer.

7) The Issuer encrypts the received encrypted share with the ECTLC-Service's public key and sends it with the device's public key to the BOPS Server A.

8) The BOPS Server A creates a DID and the DID document, and stores the DID on the Blockchain, and stores the DID document on the Identity hub.

9) The BOPS Server A sends the created DID to the Issuer.

*10)*The Issuer sends the received DID to the mobile device.

B. Authentication

1) The User creates a QR code with his DID, signature and public key into the Verifier using his mobile device and sends it to the Verifier.

2) The Verifier scans the received QR code. Should initial decoding fail (e.g., due to partial image corruption), the system initiates recursive grid-based scanning to reconstruct the SSI payload from salvageable segments. Upon successful recovery, it requests the corresponding DID document from the BOPS Server B.

3) The BOPS Server B resolves the DID and fetches the corresponding DID Document via a Blockchain from the Identity hub.

4) The BOPS Server B requests the ECTLC-Service for the ECTLC-Service's private key.

5) Upon receiving the request, the ECTLC-Service checks the time value. If the current time value has already reached the time value T, the ECTLC-Service generates a private key according to the ECTLC cryptographic protocol and sends it to the BOPS Server B. If the current time value has not yet reached the time value T, the ECTLC-Service rejects the request and sends the BOPS Server B a message that data is not available until the specified time value. And the BOPS Server B sends the corresponding message to the Verifier.

6) The BOPS Server B verifies known issuer signature and enrollment signature, and decrypts encrypted share with the received ECTLC-Service's private key.

7) The BOPS Server B requests the secured share and signed challenge from the mobile device.

8) The secured share is retrieved.

9) The User produces his biometric query template using his mobile device.

*10)*The challenge is signed with the device's private key.

*11)*The retrieved first share, query template and signed challenge are sent to the BOPS Server B.

*12)*The BOPS Server B verifies the challenge signature and decrypts the encrypted share using enrollment public key.

*13)*The BOPS Server B combines shares and performs match.

*14)*The BOPS Server B returns the match result to the Verifier and deletes shares and associated keys.

*15)*The Verifier authorizes access.

The proposed protocol enables a wide range of scenarios where time-sensitive access to identity documents and personal data, including biometrics, is required. The following are some possible use cases where delayed access is critical.

Example 1. A will with biometric confirmation after death.

The user creates a digital will encrypted using TLC and stored in a decentralized repository. The owner's biometric template (e.g., fingerprint) is shared using the Horcrux scheme. Access to the decrypted will is possible only after legal confirmation of death and the expiration of a set time interval (e.g., 30 days). This model prevents premature disclosure of the will and ensures that only authorized persons can access it.

Example 2. Medical data with access at the time of surgery.

The patient uploads preliminary consent for surgery and their medical data in encrypted form. The documents are only available at the time of surgery and are automatically activated at the appointed time via TLC. Access is only possible after the patient and medical staff have undergone biometric verification. This protects against manipulation and premature familiarization of medical information by third parties.

Example 3. A court opinion activated at a hearing.

A digital expert opinion (e.g., on biological evidence) is encrypted by TLC and published in the blockchain with an activation tag on the court date. A QR code confirming the availability and authenticity of the opinion is presented for verification in court. The expert's biometrics additionally confirm authorship, and the impossibility of disclosure before the specified deadline excludes any influence on the process.

Example 4. A digital pass with future activation.

As part of physical access to a facility (e.g., a data center), the contractor receives a VC with the right to enter, but it is activated only from a certain fixed time. The contractor's biometrics are used as a means of identity verification, and the QR code contains a link to encrypted access rights. Until activation, access is impossible, either technically or cryptographically.

V. Discussion

1) Threat model and mitigations: We consider MITM and replay; the verifier requires signed envelopes and challenge–response over authenticated channels. A single biometric share compromise does not enable reconstruction; premature disclosure is prevented by the ECTLC time barrier.

2) Limitations: Threshold availability of ECTLC participants and DID/VC revocation signaling are operational dependencies; biometric capture quality may impact FAR/FRR.

3) Applicability: Medical/legal attestations and controlled physical access where provable non-access before time (T) is a strict requirement.

VI. Conclusion

The study proposes a cryptographic protocol that expands the capabilities of Self-Sovereign Identity by supporting deferred access to data and decentralized management of biometric information. Based on a combination of the Horcrux and the Elliptic Curves Time-Lapse Cryptography protocols, the developed approach ensures a high level of privacy and security, and complete user autonomy in managing their identities. The protocol is applicable in legal, medical, educational and commercial scenarios where strict time control and provability of digital identity are required. The proposed protocol takes into account current threats in the field of digital identification and privacy of personal data. Due to the use of Time-Lapse Cryptography, data protected within the Verifiable Credential is inaccessible until the moment T specified during encryption. Even with an encrypted message, an attacker is unable to access the content until the cryptographic "delay" is complete. Instead of storing templates in centralized databases, the Horcrux protocol is used, which provides distributed storage and restoration of biometrics only by multilateral agreement. This eliminates the possibility of compromising templates even if one of the participants is hacked. The use of VC and DID signed via blockchain allows for verification of authorship and immutability of data. QR codes contain only links to data and digital fingerprints, eliminating the possibility of falsification without access to the Issuer's private key. In the future, it is planned to implement a reference implementation and detailed analysis of the protocol for performance and correctness.

Acknowledgment

The work was carried out with the financial support of the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan, No. AP19678000.

References

[1] Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity: Decentralized digital identity and verifiable credentials. Manning Publications.

[2] Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. IEEE Access, 7, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173.

[3] Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002.

[4] Harmon, J. D., Tobin, A., & Reed, D. (2019). The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON) (pp. 37–46). IEEE. https://doi.org/10.1109/DAPPCON.2019.00013.

[5] Tasmagambetov, Olzhas, Yerzhan Seitkulov, Ruslan Ospanov, and Banu Yergaliyeva. “Fault-tolerant Backup Storage System for Confidential Data in Distributed Servers.” TELKOMNIKA (Telecommunication Computing Electronics and Control) 21, no. 5 (October, 2023): 1030. https://doi.org/10.12928/telkomnika.v21i5.25305.

[6] 2410-2017 - IEEE Standard for Biometric Open Protocol Standard. IEEE. https://doi.org/10.1109/IEEESTD.2017.8089818.

[7] Cui, H., Whitty, M., Miyaji, A., Li, Z. (2025). A Blockchain-Based Digital Identity Management System via Decentralized Anonymous Credentials. In Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '24). Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3659463.3660027.

[8] Paredes-García, D., Fernández-Carrasco, J. Á., López, J. A. M., Vasquez-Correa, J. C., Yoldi, I. J., Moreno-Acevedo, S. A., González-Docasal, A., Irazusta, H. A., Muniain, A. Á., & Loinaz, Y. d. D. (2025). SIBERIA: A Self-Sovereign Identity and Multi-Factor Authentication Framework for Industrial Access. Applied Sciences, 15(15), 8589. https://doi.org/10.3390/app15158589.

[9] Saprunov, V., Muhammad, F., Kyung-Hyune, R. (2024) Privacy-Preserving Decentralized Biometric Identity Verification in Car-Sharing System. J Multimed Inf Syst 2024;11(1):17-34. https://doi.org/10.33851/JMIS.2024.11.1.17.

[10] Naicker, D., Moodley, M. (2024) Challenges of user data privacy in self-sovereign identity verifiable credentials for autonomous building access during the COVID-19 pandemic. Front. Blockchain 7:1374655. https://doi.org/10.3389/fbloc.2024.1374655.

[11] Enge, A., Satybaldy, A, Nowostawski, M. (2022) An offline mobile access control system based on self-sovereign identity standards. Computer Networks, Volume 219, 109434, https://doi.org/10.1016/j.comnet.2022.109434.

[12] Rabin, M.O., Thorpe, C.A. (2006) “Time-lapse cryptography”, Technical report TR-22-06, Harvard University School of Engineering and Computer Science.

[13] Rabin, M.O., Thorpe, C.A. (2007) “Method and apparatus for time-lapse cryptography”, U.S. Patent 8,526,621.

[14] Thorpe, C.A., Barrientos, M., Rabin, M.O. (2009) “Implementation of A Time-Lapse Cryptography Service”, IEEE Symposium on Security and Privacy, Oakland.

[15] T. P. Pedersen. A Threshold Cryptosystem without a Trusted Party. In Advances in Cryptology—Eurocrypt’91, pages 522–526. Springer-Verlag, 1991.

[16] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. IEEE Symposium on Foundations of Computer Science, pages 427–437, 1987.

[17] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Information Theory, IT-31(4):469–472, 1985.

[18] Kivinen, T. M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003, doi: https://doi.org/10.17487/RFC3526

[19] M. Lepinski, S. Kent “Additional Diffie-Hellman Groups for Use with IETF Standards”, RFC 5114, January 2008, doi: https://doi.org/10.17487/RFC5114

[20] Tang C., Chronopoulos, A.T. An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering // Proceedings of IEEE ICPADS 2005, The 11th International Conference on Parallel and Distributed Systems, 20-22 July 2005, Volume 2, Fukuoka, Japan, pp. 285 - 289.

[21] Pedersen T.P. Non-iteractive and information-theoretic secure verifiable secret sharing // In Proc. Of CRYPTO 1991, the 11th Ann. Intl. Cryptology Conf., vol. 576 of Lecture Notes in Computer Science, pp. 129–140. Aug. 1991.

[22] Trung M.M., Do L.P., Tuan D.T., Tanh N.V., Tri N.Q. Design a cryptosystem using elliptic curves cryptography and Vigenère symmetry key // IJECE, vol. 13, no. 2, pp. 1734-1743, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1734-1743.

[23] Bernstein D.J., Lange T. SafeCurves: choosing safe curves for elliptic-curve cryptography. http://safecurves.cr.yp.to

[24] Kukharev, G., Kaziyeva, N., Tsymbal, D. (2018) Barcoding Technologies for the Tasks of the Facial Biometrics: State of the Art and New Solutions. Pattern Recognition and Image Analysis, vol. 28, pp. 496-509.

[25] Soldek J. et al. (1997) Image analysis and pattern recognition in biometric technologies. In: Proc. Int. Conf. on the Biometrics: Fraud Prevention, Enhanced Service. Las Vegas, USA, pp. 270-286.

[26] Kukharev G.A., Kaziyeva N. (2019) Algorithms of color QR codes formation for biometry tasks. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2019, vol. 19, no. 5, pp. 955-958 (in Russian). doi: 10.17586/2226-1494-2019-19-5-955-958.

[27] Polygon Team, "Polygon Amoy Testnet Documentation," 2023. [Online]. Available: https://docs.polygon.technology.

[28] W3C. Verifiable Credentials Data Model v2.0. W3C Recommendation, 15 May 2025.

[29] W3C. Decentralized Identifiers (DID) v1.0. W3C Recommendation, 19 July 2022.

[30] W3C. Data Integrity BBS Cryptosuites v1.0. Candidate Recommendation Draft, 3 April 2025.

[31] ISO/IEC 24745:2022. Information technology-Security techniques - Biometric information protection.