4ª EDIÇÃO Science & Business Connection by colmeia

# Um Mecanismo Escalável de Revogação para SSI: Âncora no Ledger e Verificação Local com Bloom Filters

Edimar Veríssimo da Silva[1]; Arlindo Flavio da Conceição[2]

[1] edimar.verissimo@unifesp.br
[2] arlindo.conceicao@unifesp.br

**Resumo:** A Identidade Autossoberana (SSI) revoluciona a gestão digital ao devolver ao indivíduo o controle absoluto de suas informações. No entanto, a revogação de credenciais impõe um desafio estrutural: a capacidade técnica dos verificadores de consultar o status dos documentos de forma irrestrita permite o rastreamento não autorizado e a criação de perfis comportamentais, violando a privacidade do usuário. Diante desta vulnerabilidade, o presente trabalho tem como objetivo propor um novo e escalável mecanismo de revogação focado em garantir a privacidade temporal de forma matemática, impedindo o monitoramento histórico ou futuro do ciclo de vida da credencial sem o consentimento explícito de seu titular. Para alcançar essa meta, a metodologia inverte radicalmente o modelo de verificação passiva. O sistema implementa uma estratégia híbrida ancorada em duas estruturas criptográficas principais: o Vetor K, que é um conjunto numérico estático gravado uma única vez na blockchain, e o Vetor L, uma lista privada de tokens temporais mantida sob a custódia exclusiva do titular. Com o intuito de otimizar o armazenamento, apenas a raiz de uma Árvore de Merkle do Vetor L é inserida nos atributos da credencial. Durante o processo de validação, o titular apresenta ao verificador exclusivamente o token correspondente à janela de tempo atual e o seu respectivo caminho de Merkle, permitindo a reconstrução da chave de busca estritamente para aquele momento. A checagem efetiva de revogação ocorre fora da rede (off-ledger), utilizando Filtros de Bloom compactos hospedados em servidores externos e gerenciados por um arquivo Manifesto ancorado no Hyperledger Indy. Os resultados demonstram notável eficiência e segurança combinatória. O pacote de dados armazenado na carteira digital do usuário restringe-se a cerca de 25 kilobytes, enquanto um Filtro de Bloom de apenas 2 megabytes suporta até 300 mil revogações, propiciando validações locais instantâneas. Adicionalmente, o modelo assegura que o emissor descarte os vetores originais logo após a geração, inviabilizando riscos de custódia. Em termos de aplicação, a proposta impacta diretamente cenários reais que exigem a verificação frequente de credenciais sem comprometer direitos fundamentais de privacidade. No setor governamental, o modelo pode ser utilizado em identidades digitais, permissões, licenças e certificados públicos, impedindo que o histórico de uso do cidadão seja monitorado em cada conferência. Na saúde, o mecanismo é relevante para credenciais profissionais, certificados de vacinação, autorizações clínicas e documentos sensíveis, situações em que a consulta constante da validade poderia revelar padrões de comportamento ou dados pessoais. Na educação, a solução permite validar diplomas e históricos acadêmicos com integridade criptográfica, sem expor o estudante ao rastreamento contínuo por instituições ou empregadores. Assim, o modelo proposto

amplia a segurança e a escalabilidade da revogação em ecossistemas SSI e fortalece a viabilidade de aplicações descentralizadas em ambientes institucionais complexos, unindo auditabilidade, desempenho e proteção da privacidade. Conclui-se que o algoritmo neutraliza a vigilância em redes SSI, garantindo uma operação descentralizada, ágil, auditável e plenamente respeitosa aos direitos fundamentais de privacidade dos indivíduos.

**Palavras-chave**: Identidade Autossoberana; Privacidade Temporal; Vetor K; Filtro de Bloom; Hyperledger Indy.

4ª EDIÇÃO Science & Business Connection by colmeia
COLMEIA
PIT

# A Scalable Revocation Mechanism for SSI: Ledger Anchoring and Local Bloom Verification Filters

Edimar Veríssimo da Silva[1]; Arlindo Flavio da Conceição[2]

[1] edimar.verissimo@unifesp.br
[2] arlindo.conceicao@unifesp.br

**Abstract:** Self-Sovereign Identity (SSI) revolutionizes digital management by returning absolute control of information to the individual. However, credential revocation poses a structural challenge: the technical ability of verifiers to access the status of documents without restriction allows for unauthorized tracking and the creation of behavioral profiles, violating user privacy. Faced with this vulnerability, this work aims to propose a new and scalable revocation mechanism focused on guaranteeing temporal privacy mathematically, preventing historical or future monitoring of the credential lifecycle without the explicit consent of its holder. To achieve this goal, the methodology radically reverses the passive verification model. The system implements a hybrid strategy anchored in two main cryptographic structures: the K-Vector, a static numerical set recorded only once on the blockchain, and the L-Vector, a private list of temporal tokens held in the exclusive custody of the holder. In order to optimize storage, only the root of a Merkle Tree of the L-Vector is inserted into the credential attributes. During the validation process, the holder presents the verifier exclusively with the token corresponding to the current time window and its respective Merkle path, allowing the reconstruction of the search key strictly for that moment. The effective revocation check occurs off-ledger, using compact Bloom Filters hosted on external servers and managed by a Manifest file anchored in Hyperledger Indy. The results demonstrate remarkable efficiency and combinatorial security. The data package stored in the user's digital wallet is limited to approximately 25 kilobytes, while a Bloom Filter of only 2 megabytes supports up to 300,000 revocations, enabling instantaneous local validations. Additionally, the model ensures that the issuer discards the original vectors immediately after generation, eliminating custody risks. In terms of application, the proposal directly impacts real-world scenarios that require frequent credential verification without compromising fundamental privacy rights. In the government sector, the model can be used for digital identities, permissions, licenses, and public certificates, preventing the citizen's usage history from being monitored at each check. In healthcare, the mechanism is relevant for professional credentials, vaccination certificates, clinical authorizations, and sensitive documents, situations where constant verification of validity could reveal behavioral patterns or personal data. In education, the solution allows for the validation of diplomas and academic transcripts with cryptographic integrity, without exposing the student to continuous tracking by institutions or employers. Thus, the proposed model enhances the security and scalability of revocation in SSI ecosystems and strengthens the viability of decentralized applications in complex institutional environments, combining auditability, performance, and

privacy protection. In conclusion, the algorithm neutralizes surveillance in SSI networks, ensuring a decentralized, agile, auditable operation that fully respects the fundamental privacy rights of individuals.

**Keywords**: Self-sovereign identity; Temporal privacy; K-vector; Bloom filter; Hyperledger Indy.