The PEACE Protocol[1]

A protocol for transferable encryption rights.

Logical Mechanism LLC[2]

October 25, 2025

[1]This project was funded in Fund 14 of Project Catalyst.
[2]Contact: support@logicalmechanism.io

Contents

1 Abstract

In this report, we introduce the PEACE protocol, an ECIES-based, multi-hop, bidirectional proxy re-encryption scheme for Cardano. PEACE solves the encrypted-NFT problem by providing a decentralized, open-source protocol for transferable encryption rights, enabling creators, collectors, and developers to manage encrypted NFTs without relying on centralized decryption services. This work fills a significant gap in secure, private access to NFTs on Cardano. The PEACE protocol was funded in round 14 of Project Catalyst[1].

2 Introduction

3 Background And Preliminaries

4 Cryptographic Primitives Overview

4.1 ECIES

4.2 AES-GCM

4.3 Proxy Re-Encryption

5 Protocol Overview

5.1 Design Goals And Requirements

5.2 On-Chain And Off-Chain Architecture

5.3 Key Management And Identity

5.4 Protocol Specification

6 Security Model

6.1 Trust Model

6.1.1 Assumptions

7 Threat Analysis

7.1 Metadata Leakage

8 Limitations And Risks

8.1 Performance And On-Chain Cost

9 Conclusion

[1] https://projectcatalyst.io/funds/14/cardano-use-cases-concepts/decentralized-on-chain-data-encryption