

The PEACE Protocol¹

A protocol for transferable encryption rights.

Logical Mechanism LLC²

October 23, 2025

¹This project was funded in Fund 14 of Project Catalyst.

²Contact: support@logicalmechanism.io

Contents

1	Abstract	1
2	Introduction	1
3	Background And Preliminaries	1
4	Cryptographic Primitives Overview	1
4.1	ECIES	1
4.2	AES-GCM	1
4.3	Proxy Re-Encryption	1
5	Protocol Overview	1
5.1	Design Goals And Requirements	1
5.2	On-Chain And Off-Chain Architecture	1
5.3	Key Management And Identity	1
5.4	Protocol Specification	1
6	Security Model	1
6.1	Trust Model	1
7	Threat Analysis	1
7.1	Metadata Leakage	1
8	Limitations And Risks	1
8.1	Performance And On-Chain Cost	1
9	Conclusion	1

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.

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