

SRS - MidnightZK Off-Ramp SDK: ADA↔Web2 Payments (Cash App, Wise)

1. Introduction

1.1 Purpose

This document specifies the functional, non-functional, privacy, and compliance requirements for the Nucast ADA Off-Ramp SDK.

1.2 Intended Audience

- Cardano developers
- Wallet providers
- Auditors
- Catalyst reviewers

1.3 Definitions

- **SDK:** Software Development Kit
- **ZKP:** Zero-Knowledge Proof
- **Off-Ramp:** Conversion of crypto to fiat
- **Escrow:** Smart contract holding funds temporarily

2. System Overview

The system consists of:

- On-chain Cardano smart contracts
- Off-chain SDK & API layer
- ZK proof generation & verification

- External payment platform connectors
-

3. User Stories

US-1: End User Off-Ramp

| As an ADA holder, I want to off-ramp ADA into my Cash App account privately without giving up custody.

US-2: Wallet Integration

| As a wallet developer, I want to integrate ADA off-ramps using a simple SDK.

US-3: Privacy Preservation

| As a user, I want my transaction details hidden from public view.

4. Functional Requirements

FR-1 Wallet-Initiated Off-Ramp

- Users initiate off-ramps from their own wallet
- No custody of funds by Nucast

FR-2 Smart Contract Escrow

- ADA locked in escrow until off-chain confirmation
- Automatic release or refund

FR-3 ZK Proof Generation

- Generate Midnight ZK proofs for:
 - Payee validity
 - Amount correctness
- No exposure of personal data

FR-4 Payment Platform Integration

- Support:
 - Cash App
 - Wise
 - Revolut
- Modular adapter architecture

FR-5 SDK APIs

- `initiateOffRamp()`
 - `generateZKProof()`
 - `submitPayment()`
 - `confirmSettlement()`
-

5. Non-Functional Requirements

NFR-1 Security

- No plaintext storage of sensitive data
- Auditable contracts

NFR-2 Performance

- Proof generation < 50 seconds
- Settlement confirmation < 7 minutes (testnet)

NFR-3 Scalability

- Stateless SDK components
- Horizontal scaling

NFR-4 Usability

- Minimal integration steps

- Clear error handling
-

6. Compliance & Regulatory Considerations

- No custody of fiat or crypto
 - Privacy-by-design architecture
 - Optional KYC hooks (jurisdiction-dependent)
 - AML triggers limited to hashed identifiers
-

7. Zero-Knowledge Privacy Parameters

| Parameter | Description |
|-------------------|---------------|
| Proof Type | Midnight ZK |
| On-Chain Data | Hashes only |
| Off-Chain Storage | Encrypted |
| Verifiability | Deterministic |
