Digital Key Generation Validator Logic

Overview

This Plutus based smart contract is designed to manage and secure the digital check-in process by creating a secure digital key for the guests. It ensures a strict and verifiable sequence of actions, involving both a guest and an administrator to guarantee that identity verification, digital key issuance and validation occur securely and transparently.

Data Structures

Datum:GuestDatum

Field	Type	Description
guestAddress	BuiltinByteString	Guest's address.
initiateCheckIn	Bool	Check if guests can opt for pre-checkin process or not.
digitalKey	BuiltinByteString	Holds a generated digital key.
isDigitalKeyValidated	BuiltinByteString	Check if generated digital key is validated by the admin or not.

Redeemer:

Defines the actions being validated:

- DigitalKeyGeneration
- DigitalKeyValidation

Validation Logic by Redeemer

1. DigitalKeyGeneration

Actor: Admin

Action: Admin will check if initiateCheckin field is true then generation of digital key will happen.

Preconditions:

- The initiateCheckIn shall be true .

Expected changes:

- Digital Key will be generated and it will assign to the field digitalKey of the guestDatum.
- Other fields will remain unchanged.

2. DigitalKeyValidation

Actor: Admin

Action: Digital key is validated.

Preconditions:

- IsDigitalKeyValidated has its default value.
- digitalKey field should have generated key as value.

Expected changes:

- Admin will set the isDigitalKeyValidated to true.