



RNS ID (RNSId) Token

Smart Contract Audit

- RNS ID (RNSId) Token Audit Summary
- RNS ID (RNSId) Token Audit
 - Document information
 - Audit results
 - Audited target file
 - Vulnerability analysis
 - Vulnerability distribution
 - Summary of audit results
 - Contract file
 - Analysis of audit results
 - Re-Entrancy
 - Arithmetic Over/Under Flows
 - Unexpected Blockchain Currency
 - Delegatecall
 - Default Visibilities
 - Entropy Illusion
 - External Contract Referencing
 - Unsolved TODO comments
 - Short Address/Parameter Attack
 - Unchecked CALL Return Values
 - Race Conditions / Front Running
 - Denial Of Service (DOS)
 - Block Timestamp Manipulation
 - Constructors with Care
 - Unintialised Storage Pointers
 - Floating Points and Numerical Precision
 - tx.origin Authentication
 - Permission restrictions

RNS ID (RNSId) Token Audit Summary

Project name : RNS ID (RNSId) Token Contract

Project address: None

Code URL : https://github.com/rick20220222/id_nft_contract

Commit : 6cb8e9bdbdb76754969ba2602bda267c1395df0b

Project target : RNS ID (RNSId) Token Contract Audit

Blockchain : Binance Smart Chain (BSC)

Test result : PASSED

Audit Info

Audit NO : 0X202305110007

Audit Team : Armors Labs

Audit Proofreading: <https://armors.io/#project-cases>

RNS ID (RNSId) Token Audit

The RNS ID (RNSId) Token team asked us to review and audit their RNS ID (RNSId) Token contract. We looked at the code and now publish our results.

Here is our assessment and recommendations, in order of importance.

Document information

Name	Auditor	Version	Date
RNS ID (RNSId) Token Audit	Rock, Sophia, Rushairer, Rico, David, Alice	1.0.1	2023-05-11

Audit results

Warning:

- The `authorizeMint` and `airdrop` interfaces have blacklist restrictions.
- RNSId is an upgradable ERC721 contract.
- It relies on version 4.8.0-rc.1 of @openzeppelin/contracts-upgradeable. Note that "rc" denotes a release candidate version, and it is recommended to use stable versions (The project team has updated to the stable version)
- The `authorizeMint` interface does not provide change for excessive payment.
- In the `_beforeTokenTransfer` hook method for [transfers, minting, and burning], users who hold tokens are unable to authorize transfers and also unable to trade.

- The tokenURI points to a centralized location.

The issues mentioned above have been confirmed by the project team.

Note that as of the date of publishing, the above review reflects the current understanding of known security patterns as they relate to the RNS ID (RNSId) Token contract. The above should not be construed as investment advice.

Based on the widely recognized security status of the current underlying blockchain and smart contract, this audit report is valid for 3 months from the date of output.

Disclaimer

Armors Labs Reports is not and should not be regarded as an "approval" or "disapproval" of any particular project or team. These reports are not and should not be regarded as indicators of the economy or value of any "product" or "asset" created by any team. Armors do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc'...)

Armors Labs Reports represent an extensive auditing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Armors does not guarantee the safety or functionality of the technology agreed to be analyzed.

Armors Labs postulates that the information provided is not missing, tampered, deleted or hidden. If the information provided is missing, tampered, deleted, hidden or reflected in a way that is not consistent with the actual situation, Armors Labs shall not be responsible for the losses and adverse effects caused. Armors Labs Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

Audited target file

file	md5
./RNSId.sol	6c037dcc687c365dc5327f0fcace018a

Vulnerability analysis

Vulnerability distribution

vulnerability level	number
Critical severity	0
High severity	0
Medium severity	0
Low severity	0

Summary of audit results

Vulnerability	status
Re-Entrancy	safe

Vulnerability	status
Arithmetic Over/Under Flows	safe
Unexpected Blockchain Currency	safe
Delegatecall	safe
Default Visibilities	safe
Entropy Illusion	safe
External Contract Referencing	safe
Short Address/Parameter Attack	safe
Unchecked CALL Return Values	safe
Race Conditions / Front Running	safe
Denial Of Service (DOS)	safe
Block Timestamp Manipulation	safe
Constructors with Care	safe
Uninitialised Storage Pointers	safe
Floating Points and Numerical Precision	safe
tx.origin Authentication	safe
Permission restrictions	safe

Contract file

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.12;

import '@openzeppelin/contracts-upgradeable/token/ERC721/ERC721Upgradeable.sol';
import '@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721EnumerableUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721MetadataUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721EnumerableUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721BurnableUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/token/ERC721/IERC721Upgradeable.sol';
import '@openzeppelin/contracts-upgradeable/token/ERC721/IERC721ReceiverUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/utils/introspection/ERC165Upgradeable.sol';
import '@openzeppelin/contracts-upgradeable/utils/introspection/IERC165Upgradeable.sol';
import '@openzeppelin/contracts-upgradeable/utils/math/SafeMathUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/security/ReentrancyGuardUpgradeable.sol';
import '@openzeppelin/contracts-upgradeable/access/AccessControlUpgradeable.sol';

contract RNSId is
    ERC721Upgradeable,
    ERC721EnumerableUpgradeable,
    ERC721BurnableUpgradeable,
    AccessControlUpgradeable,
    ReentrancyGuardUpgradeable
{
    using SafeMathUpgradeable for uint256;
```

```

event RNSAddressAuthorized(string _rnsId, address indexed _wallet);
event RNSNewID(string _rnsId, address indexed _wallet, uint256 _tokenId);
event RNSBurnID(string _rnsId, address indexed _wallet, uint256 _tokenId);

uint256 public mintPrice;
uint256 public lastTokenId;
string private baseURI;
address private destination;

// do any admin operations but receive fund
bytes32 public constant SECONDARY_ADMIN_ROLE = keccak256('SECONDARY_ADMIN_ROLE');

mapping(string => bool) public isMinted;
mapping(string => bool) public isAuthorized;
mapping(string => uint256) public numMinted;
mapping(address => bool) private isBlockedAddress;
mapping(string => bool) private isBlockedRnsID;

// Metadata for ID NFT
mapping(uint256 => bytes32) public tokenIdToMerkle;
mapping(uint256 => address) public tokenIdToWallet;
mapping(uint256 => string) public tokenIdToRnsId;

function initialize() public initializer {
    __ERC721_init('RNS ID', 'RNSId');

    // todo: update price; Brill and team please decide mintPrice
    mintPrice = 0.01 ether;

    // todo: change to prod
    baseURI = 'https://api.rns.id/api/v2/portal/identity/nft/';
    __AccessControl_init();
    __grantRole(DEFAULT_ADMIN_ROLE, msg.sender);
    __grantRole(SECONDARY_ADMIN_ROLE, msg.sender);
    // set contract deployer to be admin role of default and secondary admin role
    __setRoleAdmin(DEFAULT_ADMIN_ROLE, DEFAULT_ADMIN_ROLE);
    __setRoleAdmin(SECONDARY_ADMIN_ROLE, DEFAULT_ADMIN_ROLE);
    destination = msg.sender;
}

function getIdentityKey(string memory _rnsId, address _wallet) internal pure returns (string memory) {
    return string(abi.encodePacked(_rnsId, string(abi.encodePacked(_wallet))));
}

function setMintPrice(uint256 _mintPrice) external onlyRole(SECONDARY_ADMIN_ROLE) {
    mintPrice = _mintPrice;
}

function setBaseURI(string memory _URI) external onlyRole(SECONDARY_ADMIN_ROLE) {
    baseURI = _URI;
}

function setIsBlockedAddress(address _wallet, bool _isBlocked) public onlyRole(SECONDARY_ADMIN_ROLE) {
    isBlockedAddress[_wallet] = _isBlocked;
}

function setIsBlockedRnsID(string memory _rnsId, bool _isBlocked) public onlyRole(SECONDARY_ADMIN_R
    isBlockedRnsID[_rnsId] = _isBlocked;
}

function setTokenIdToMerkle(uint256 tokenId, bytes32 _merkelRoot) external onlyRole(SECONDARY_ADMIN
    tokenIdToMerkle[tokenId] = _merkelRoot;
}

function authorizeMint(string memory _rnsId, address _wallet) external payable nonReentrant {

```



```

string memory idAddressKey = getIdentityKey(_rnsId, _wallet);
require(!isAuthorized[idAddressKey], 'already authorized an ID for the address');
require(!isBlockedAddress[_wallet], 'the wallet is blacklisted');
require(!isBlockedRnsID[_rnsId], 'the RNS ID is blacklisted');
uint256 fee = mintPrice;
uint256 numMintedForID = numMinted[_rnsId];
if (hasRole(SECONDARY_ADMIN_ROLE, msg.sender)) {
    fee = 0;
}
require(msg.value >= fee, 'insufficient fund');
numMinted[_rnsId] = numMintedForID.add(1);
isAuthorized[idAddressKey] = true;
emit RNSAddressAuthorized(_rnsId, _wallet);
}

function airdrop(
    string memory _rnsId,
    address _wallet,
    bytes32 _merkleRoot
) external onlyRole(SECONDARY_ADMIN_ROLE) nonReentrant {
    string memory idAddressKey = getIdentityKey(_rnsId, _wallet);
    require(!isMinted[idAddressKey], 'already minted an ID for the address');
    require(!isBlockedAddress[_wallet], 'the wallet is blacklisted');
    require(!isBlockedRnsID[_rnsId], 'the RNS ID is blacklisted');
    isMinted[idAddressKey] = true;
    uint256 tokenId = lastTokenId.add(1);
    lastTokenId = tokenId;

    _safeMint(_wallet, tokenId);

    tokenIdToMerkle[tokenId] = _merkleRoot;
    tokenIdToWallet[tokenId] = _wallet;
    tokenIdToRnsId[tokenId] = _rnsId;

    emit RNSNewID(_rnsId, _wallet, tokenId);
}

function _baseURI() internal view virtual override returns (string memory) {
    return baseURI;
}

function tokenURI(uint256 tokenId) public view virtual override returns (string memory) {
    _requireMinted(tokenId);
    return bytes(baseURI).length > 0 ? string(abi.encodePacked(baseURI, tokenIdToRnsId[tokenId], '.js')) : '';
}

function tokenMerkleRoot(uint256 tokenId) public view virtual returns (bytes32) {
    _requireMinted(tokenId);

    return tokenIdToMerkle[tokenId];
}

function setFundDestination(address _destination) public onlyRole(DEFAULT_ADMIN_ROLE) {
    destination = _destination;
}

function withdraw() public onlyRole(DEFAULT_ADMIN_ROLE) {
    payable(destination).transfer(address(this).balance);
}

function supportsInterface(
    bytes4 _interfaceId
) public view override(ERC721Upgradeable, ERC721EnumerableUpgradeable, AccessControlUpgradeable) reverts {
    return super.supportsInterface(_interfaceId);
}

```

```

function burn(uint256 _tokenId) public override(ERC721BurnableUpgradeable) {
    super.burn(_tokenId);
    emit RNSBurnID(tokenIdToRnsId[_tokenId], tokenIdToWallet[_tokenId], _tokenId);
}

function _beforeTokenTransfer(
    address from, address to, uint256 firstTokenId, uint256 batchSize
) internal virtual override(ERC721Upgradeable, ERC721EnumerableUpgradeable) {
    if (from != address(0)) {
        address owner = ownerOf(firstTokenId);
        require(owner == msg.sender, 'Only the owner of NFT can transfer or burn it');
        require(to == address(0) || from == address(0), 'an RnsID NFT can only be airdropped or burned');
    }
    super._beforeTokenTransfer(from, to, firstTokenId, batchSize);
}
}

```

Analysis of audit results

Re-Entrancy

- **Description:**

One of the features of smart contracts is the ability to call and utilise code of other external contracts. Contracts also typically handle Blockchain Currency, and as such often send Blockchain Currency to various external user addresses. The operation of calling external contracts, or sending Blockchain Currency to an address, requires the contract to submit an external call. These external calls can be hijacked by attackers whereby they force the contract to execute further code (i.e. through a fallback function), including calls back into itself. Thus the code execution "re-enters" the contract. Attacks of this kind were used in the infamous DAO hack.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Arithmetic Over/Under Flows

- **Description:**

The Virtual Machine (EVM) specifies fixed-size data types for integers. This means that an integer variable, only has a certain range of numbers it can represent. A uint8 for example, can only store numbers in the range [0,255]. Trying to store 256 into a uint8 will result in 0. If care is not taken, variables in Solidity can be exploited if user input is unchecked and calculations are performed which result in numbers that lie outside the range of the data type that stores them.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unexpected Blockchain Currency

- **Description:**

Typically when Blockchain Currency is sent to a contract, it must execute either the fallback function, or another function described in the contract. There are two exceptions to this, where Blockchain Currency can exist in a contract without having executed any code. Contracts which rely on code execution for every Blockchain Currency sent to the contract can be vulnerable to attacks where Blockchain Currency is forcibly sent to a contract.

- **Detection results:**

PASSED!

- **Security suggestion:** no.

Delegatecall

- **Description:**

The CALL and DELEGATECALL opcodes are useful in allowing developers to modularise their code. Standard external message calls to contracts are handled by the CALL opcode whereby code is run in the context of the external contract/function. The DELEGATECALL opcode is identical to the standard message call, except that the code executed at the targeted address is run in the context of the calling contract along with the fact that msg.sender and msg.value remain unchanged. This feature enables the implementation of libraries whereby developers can create reusable code for future contracts.

- **Detection results:**

PASSED!

- **Security suggestion:** no.

Default Visibilities

- **Description:**

Functions in Solidity have visibility specifiers which dictate how functions are allowed to be called. The visibility determines whether a function can be called externally by users, by other derived contracts, only internally or only externally. There are four visibility specifiers, which are described in detail in the Solidity Docs. Functions default to public allowing users to call them externally. Incorrect use of visibility specifiers can lead to some devastating vulnerabilities in smart contracts as will be discussed in this section.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Entropy Illusion

- **Description:**

All transactions on the blockchain are deterministic state transition operations. Meaning that every transaction modifies the global state of the ecosystem and it does so in a calculable way with no uncertainty. This ultimately means that inside the blockchain ecosystem there is no source of entropy or randomness. There is no rand()

function in Solidity. Achieving decentralised entropy (randomness) is a well established problem and many ideas have been proposed to address this (see for example, RandDAO or using a chain of Hashes as described by Vitalik in this post).

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

External Contract Referencing

- **Description:**

One of the benefits of the global computer is the ability to re-use code and interact with contracts already deployed on the network. As a result, a large number of contracts reference external contracts and in general operation use external message calls to interact with these contracts. These external message calls can mask malicious actors intentions in some non-obvious ways, which we will discuss.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unsolved TODO comments

- **Description:**

Check for Unsolved TODO comments

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Short Address/Parameter Attack

- **Description:**

This attack is not specifically performed on Solidity contracts themselves but on third party applications that may interact with them. I add this attack for completeness and to be aware of how parameters can be manipulated in contracts.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unchecked CALL Return Values

- **Description:**

There a number of ways of performing external calls in solidity. Sending Blockchain Currency to external accounts is commonly performed via the transfer() method. However, the send() function can also be used and, for more versatile external calls, the CALL opcode can be directly employed in solidity. The call() and send() functions return a boolean indicating if the call succeeded or failed. Thus these functions have a simple caveat, in that the transaction that executes these functions will not revert if the external call (intialised by call() or send()) fails, rather the call() or send() will simply return false. A common pitfall arises when the return value is not checked, rather the developer expects a revert to occur.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Race Conditions / Front Running

- **Description:**

The combination of external calls to other contracts and the multi-user nature of the underlying blockchain gives rise to a variety of potential Solidity pitfalls whereby users race code execution to obtain unexpected states. Re-Entrancy is one example of such a race condition. In this section we will talk more generally about different kinds of race conditions that can occur on the blockchain. There is a variety of good posts on this subject, a few are: Wiki - Safety, DASP - Front-Running and the Consensus - Smart Contract Best Practices.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Denial Of Service (DOS)

- **Description:**

This category is very broad, but fundamentally consists of attacks where users can leave the contract inoperable for a small period of time, or in some cases, permanently. This can trap Blockchain Currency in these contracts forever, as was the case with the Second Parity MultiSig hack

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Block Timestamp Manipulation

- **Description:**

Block timestamps have historically been used for a variety of applications, such as entropy for random numbers (see the Entropy Illusion section for further details), locking funds for periods of time and various state-changing conditional statements that are time-dependent. Miner's have the ability to adjust timestamps slightly which can prove to be quite dangerous if block timestamps are used incorrectly in smart contracts.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Constructors with Care

- **Description:**

Constructors are special functions which often perform critical, privileged tasks when initialising contracts. Before solidity v0.4.22 constructors were defined as functions that had the same name as the contract that contained them. Thus, when a contract name gets changed in development, if the constructor name isn't changed, it becomes a normal, callable function. As you can imagine, this can (and has) lead to some interesting contract hacks.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Unintialised Storage Pointers

- **Description:**

The EVM stores data either as storage or as memory. Understanding exactly how this is done and the default types for local variables of functions is highly recommended when developing contracts. This is because it is possible to produce vulnerable contracts by inappropriately initialising variables.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Floating Points and Numerical Precision

- **Description:**

As of this writing (Solidity v0.4.24), fixed point or floating point numbers are not supported. This means that floating point representations must be made with the integer types in Solidity. This can lead to errors/vulnerabilities if not implemented correctly.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

tx.origin Authentication

- **Description:**

Solidity has a global variable, tx.origin which traverses the entire call stack and returns the address of the account that originally sent the call (or transaction). Using this variable for authentication in smart contracts leaves the contract vulnerable to a phishing-like attack.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Permission restrictions

- **Description:**

Contract managers who can control liquidity or pledge pools, etc., or impose unreasonable restrictions on other users.

- **Detection results:**

PASSED!

- **Security suggestion:**

no.

Armors Labs

armors.io

contact@armors.io

