CERTIK

Audit Report

Produced by CertiK

for

Nov 21, 2019

CertiK Audit Report For MyKey

Request Date: 2019-08-28
Revision Date: 2019-11-20
Platform Name: Ethereum

CERTIK

Contents

Disclaimer 1

About CertiK 2

Executive Summary 3

Vulnerability Classification 3

Testing Summary 4
Audit Score 4
Type of Issues 4
Vulnerability Details 5

Manual Review Notes 6

Static Analysis Results 19

Formal Verification Results 24
How to read 24

Source Code with CertiK Labels 43

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Verification Services Agreement between CertiK and MyKey(the “Company”), or the scope of services/verification, and terms and conditions provided to the Company in connection with the verification (collectively, the “Agreement”). This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK’s prior written consent.

About CertiK

CertiK is a technology-led blockchain security company founded by Computer Science professors from Yale University and Columbia University built to prove the security and correctness of smart contracts and blockchain protocols.

CertiK, in partnership with grants from IBM and the Ethereum Foundation, has developed a proprietary Formal Verification technology to apply rigorous and complete mathematical reasoning against code. This process ensures algorithms, protocols, and business functionalities are secured and working as intended across all platforms.

CertiK differs from traditional testing approaches by employing Formal Verification to mathematically prove blockchain ecosystem and smart contracts are hacker-resistant and bug-free. CertiK uses this industry-leading technology together with standardized test suites, static analysis, and expert manual review to create a full-stack solution for our partners across the blockchain world to secure 6.2B in assets.

For more information: https://certik.org/

Executive Summary

This report has been prepared for MyKey to discover issues and vulnerabilities in the source code of their smart contracts. A comprehensive examination has been performed, utilizing CertiK's Formal Verification Platform, Static Analysis, and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practice and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line by line manual review of the entire codebase by industry experts.

Vulnerability Classification

CertiK categorizes issues into 3 buckets based on overall risk levels:

Critical

The code implementation does not match the specification, or it could result in the loss of funds for contract owner or users.

Medium

The code implementation does not match the specification under certain conditions, or it could affect the security standard by lost of access control.

Low

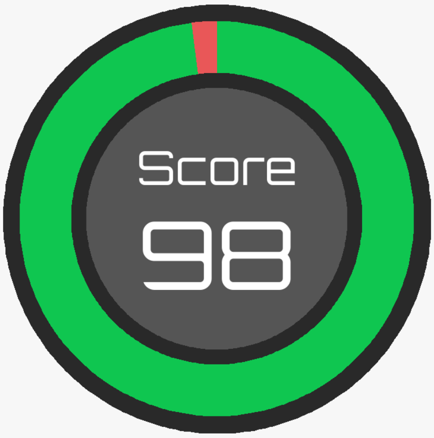
The code implementation does not follow best practices, or use suboptimal design patterns, which may lead to security vulnerabilities further down the line.

Testing Summary

PASS

CERTIK *believes this smart contract passes security qualifications to be listed on digital asset exchanges.*

Nov 20, 2019



Type of Issues

CertiK smart label engine applied 100% formal verification coverage on the source code. Our team of engineers has scanned the source code using our proprietary static analysis tools and code-review methodologies. The following technical issues were found:

Title	Description	Issues	SWC ID
Integer Overflow and Underflow	An overflow/underflow happens when an arithmetic operation reaches the maximum or minimum size of a type.	0	SWC-101
Function incorrectness	Function implementation does not meet the specification, leading to intentional or unintentional vulnerabilities.	0	
Buffer Overflow	An attacker is able to write to arbitrary storage locations of a contract if array of out bound happens	0	SWC-124
Reentrancy	A malicious contract can call back into the calling contract before the first invocation of the function is finished.	0	SWC-107
Transaction Order Dependence	A race condition vulnerability occurs when code depends on the order of the transactions submitted to it.	0	SWC-114
Timestamp Dependence	Timestamp can be influenced by miners to some degree.	1	SWC-116
Insecure Compiler Version	Using an fixed outdated compiler version or floating pragma can be problematic, if there are publicly disclosed bugs and issues that affect the current compiler version used.	1	SWC-102 SWC-103
Insecure Randomness	Block attributes are insecure to generate random numbers, as they can be influenced by miners to some degree.	0	SWC-120

"tx.origin" for authorization	tx.origin should not be used for authorization. Use msg.sender instead.	0	SWC-115
Delegatecall to Untrusted Callee	Calling into untrusted contracts is very dangerous, the target and arguments provided must be sanitized.	0	SWC-112
State Variable Default Visibility	Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.	0	SWC-108
Function Default Visibility	Functions are public by default. A malicious user is able to make unauthorized or unintended state changes if a developer forgot to set the visibility.	0	SWC-100
Uninitialized variables	Uninitialized local storage variables can point to other unexpected storage variables in the contract.	0	SWC-109
Assertion Failure	The assert() function is meant to assert invariants. Properly functioning code should never reach a failing assert statement.	0	SWC-110
Deprecated Solidity Features	Several functions and operators in Solidity are deprecated and should not be used as best practice.	0	SWC-111
Unused variables	Unused variables reduce code quality	0	

Vulnerability Details

Critical

No issue found.

Medium

No issue found.

Low

No issue found.

Manual Review Notes

Review Details

MyKey, a Self-sovereign Identity System built on various public blockchains. It mission is building a one-stop digital life platform for users through digital currency storage, trading, wealth management, games and community, and builds a variety of businesses for developers. The model's blockchain application development and operation ecosystem. In MyKey, users can control their assets autonomously, and when they lose their account, they can easily freeze and recover their accounts. In addition, MyKey is also part of the Web of Trust. In the Web 3.0, MyKey returns the data sovereignty to the user, which fundamentally protects the user's privacy rights.
MyKey Smart Contract Wallet provides following features such as:

- Creating wallet
- Signing a transaction
- Multi-signing
- Managing crypto assets
- Submitting proposals
- Restoring key

Scope of Audit

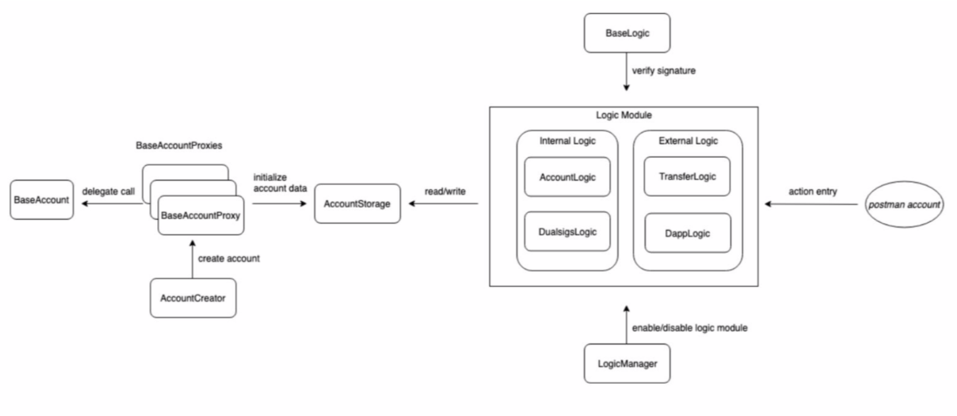
CertiK was chosen by MyKey to audit the design and implementation of its soon to be released smart contract. To ensure comprehensive protection,the source code has been analyzed by the proprietary CertiK formal verification engine and manually reviewed by our smart contract experts and engineers. That end-to-end process ensures proof of stability as well as a hands-on, engineering-focused process to close potential loopholes and recommend design changes in accordance with the best practices in the space.

Source Code SHA-256 Checksum

- **Account.sol**
  `d91ec9f494b653d3bc32421a1d520605c05bc0a69f8be423bec2bff711980aed`
- **AccountCreator.sol**
  `ad10eed20a6257849749eebdecd68c10c00be520687e61b087dba2052392731f`
- **AccountProxy.sol**
  `f334c7926ba32f68f52c64f01ac1d03b7ccdb7f5e88e664a449724b7e81c0dbf`
- **AccountStorage.sol**
  `f8e378640f804e688113395bb1c2baef73c6b6560bbf3667c6940b0cb16892bb`
- **LogicManager.sol**
  `6aa62a6699366d53543b2c1310809b39d818b8beb4296fad7554e49c0c3259c1`

- **AccountLogic.sol**
  `411f989b3a711b48ce12dc3c9966f9e8bbd25a720dbbb48859f8db4a3b40eb95`
- **DappLogic.sol**
  `8645237e508efaa6cd9073326a983295ffc413f62bf4ceb3bdb5f1d9fa94def3`
- **DualsigsLogic.sol**
  `d034a96a40b4bd187b3b4aa69ff66b59ff8a0398f82c35365abd66d93aa81bb7`
- **TransferLogic.sol**
  `a12db02a56cdede96e637f5aca9cc226d3c7023c3c75eef4b835c14176d76c8d`
- **AccountBaseLogic.sol**
  `ca6ffe59e4e1e2ecc017e6c8d286f195b9e4e67f86ad0b58728465b154f2f268`
- **BaseLogic.sol**
  `6cfe9c8990d8c63fc95c4e505ddd0e0f2c83dc664e72f61f640c85a2c765d714`
- **MyNft.sol**
  `b41eb4f8d4f96722562e31d68c15e5e224c771342680379954f51ce4fbbb8b4d`
- **MyToken.sol**
  `ad67e648646af505fc51152dd2d1cf81e4f5bf139a5b55cd1104e3cbfa5042a2`
- **MultiOwned.sol**
  `51d174dc864e45d2fefb3551aab784320b34f3dedb2c75be789274df8d827df1`
- **Owned.sol**
  `9c3fe9adaedbbe27940e0f25c27c3d8e5811a3d3ad658e4d058a1840afcef09e`
- **SafeMath.sol**
  `8f5ffacb100244d0da64f334543c3298be1c48a7ce9aadae06516c5e01f47714`

MyKey Architect & Workflow Overview



System Overview:

1. For each MyKey account will provide an corresponding `Account Proxy` contract address (Not an externally owned account)

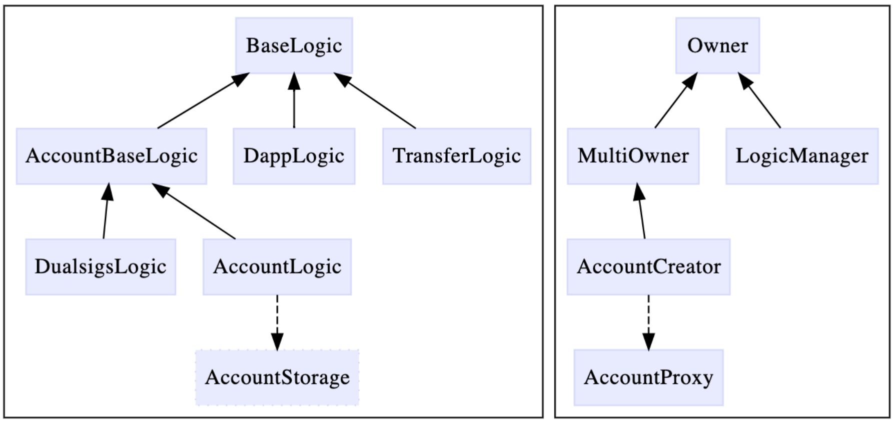
2. While creating a new MyKey account, `MyKey Lab` will set as one of the backup keys as default setting, users can add more backup keys later.

3. All MyKey user related data will storage in contract `AccountStorage`, for instance account admin key, 6(max) backup operation keys, delayItem and multi-sign Proposal Items

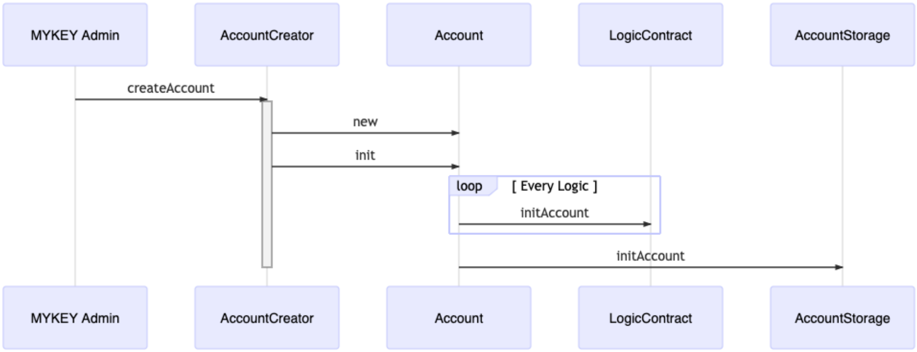
4. Logic Modules, including all the contract logic such as transfer, multi-signing proposal, dapp, and account related logic

5. LogicManager, as named handling all the logic contracts upgradeability, allow contracts to be upgraded due to its business expansion, and vulnerability fixes etc...

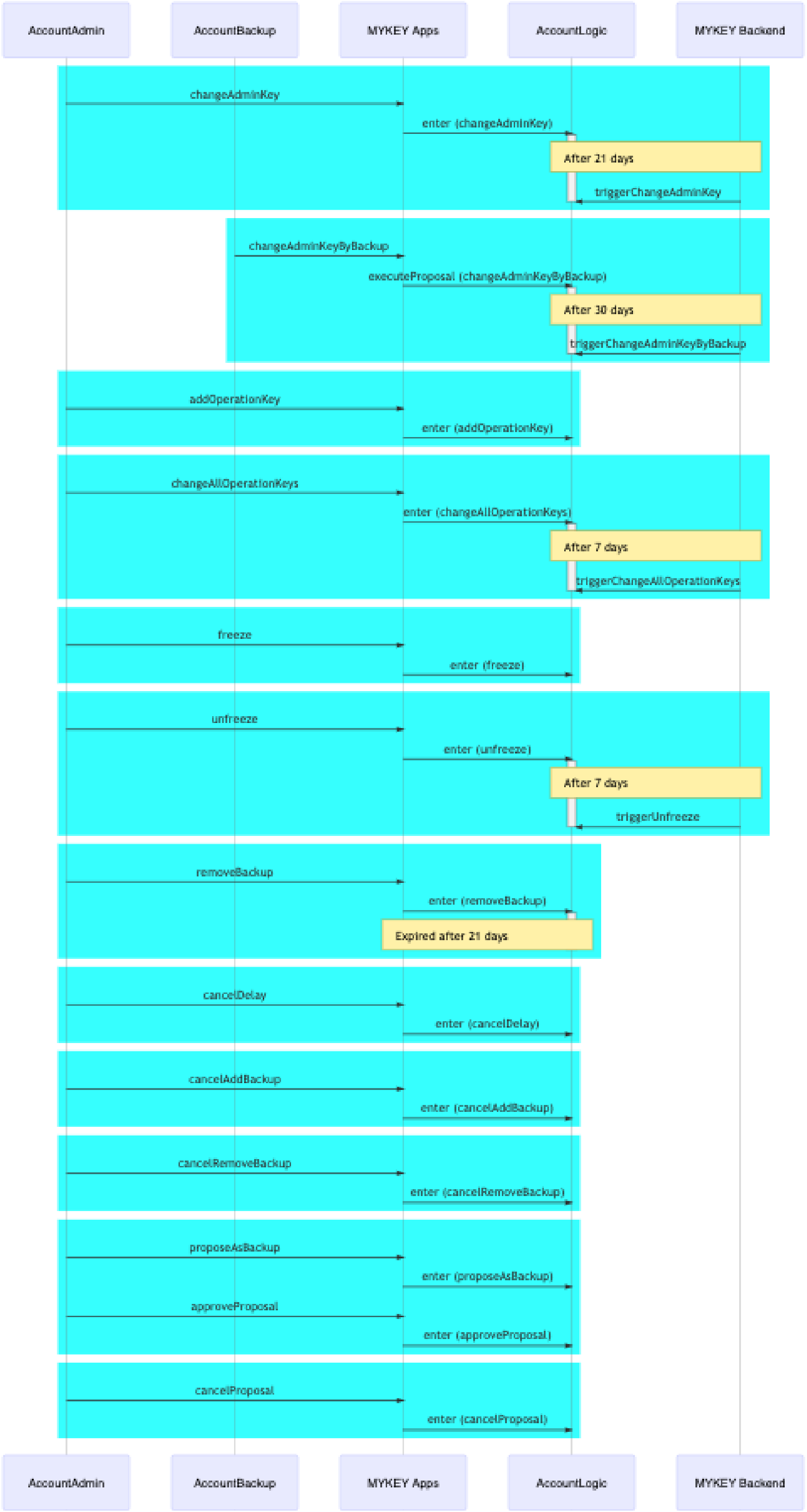
MyKey team provide the smart contract wallet design architecture diagram, each module workflow process can be illustrate as following:



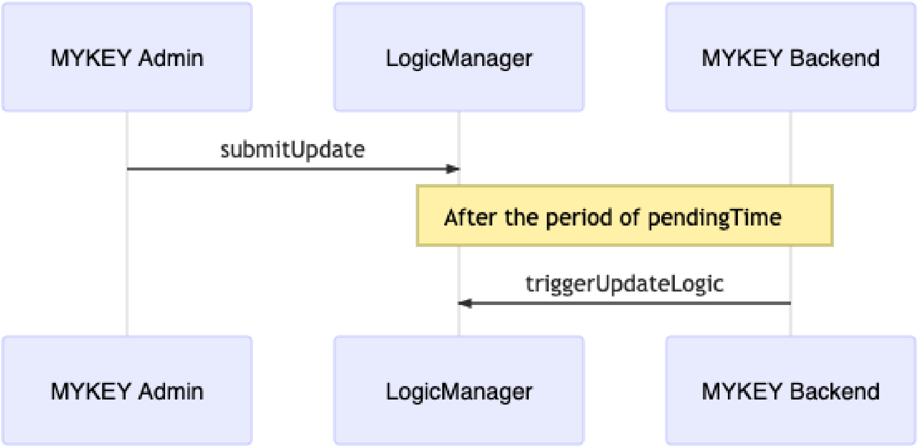
Account Creation Workflow



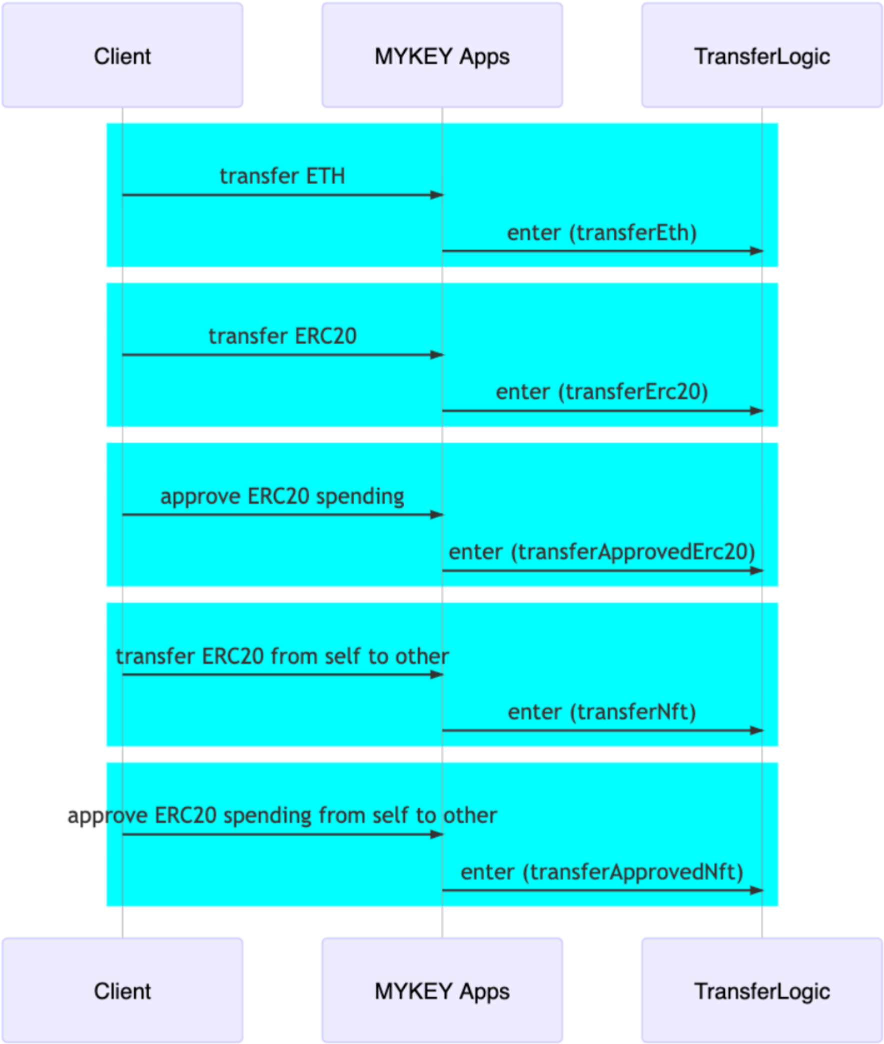
Account Logic Workflow



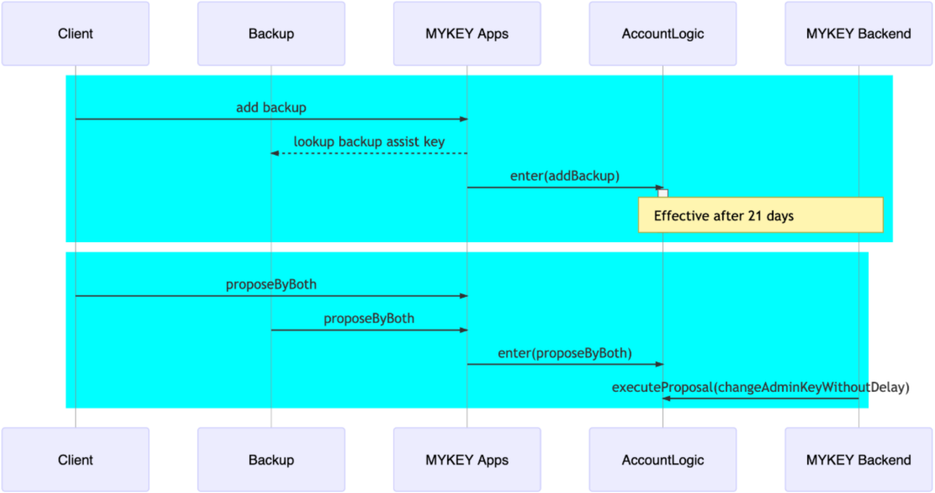
Account Logic Update Workflow



Account Logic Transfer Workflow



Account Logic Dualsig Workflow



Review Comments

BasicLogic.sol

- INFO Consider using `enum` for `ENVIRONMENT` type for better readability.
  - ✓ MyKey The `ENVIRONMENT` type is removed on production.
- MINOR `getSignHash()` Recommend declaring the `prefix` variable as a constant for gas optimization.
  - ✓ MyKey The code is updated and reflected in the latest commit
- MINOR `verifySig()` Recommend checking the `_signature` length is 65 `require(_signature.length == 65, ''invalid _signature length'')`
  - ✓ MyKey The code is updated and reflected in the latest commit
- MINOR `verifySig()` The `signatureSplit()` mentioned the `bytes is not working due to the Solidity parser` would you mind to share any references or case failure examples?
  - ✓ MyKey The `signatureSplit()` is removed and updated to `recover()` and reflected in the latest commit.
- MINOR `checkAndUpdateNonce()` Consider using SafeMath library for adding `now` + 86400 to prevent the issue cause by integer underflow or overflow

AccountCreator.sol

- INFO `constructor()` Recommend to check the variables `_mgr`, `_storage`, `_accountImpl` are not an zero address for minimizing the human errors.
- MINOR Given `close()` will invoke `selfdestruct`, a very low-level opcode call, highly recommend to emit an event for future reference as a best practice.
  - ✓ MyKey The code is updated and reflected in the latest commit.

AccountLogic.sol

- INFO Recommend to remove the declaration of `actionId` variable, instead use the constant variable directly.

  1. `changeAllOperationKeys`
  2. `triggerChangeAdminKeyByBackup`
  3. `changeAllOperationKeys`
  4. `triggerChangeAllOperationKeys`
  5. ✓ MyKey The code is updated and reflected in the latest commit.

- MINOR Recommend declaring the local memory variable outside the for loop for gas optimization.

  1. `changeAllOperationKeys`
  2. `triggerChangeAdminKeyByBackup`
  3. `changeAllOperationKeys`
  4. `triggerChangeAllOperationKeys`
  5. ✓ MyKey The code is updated and reflected in the latest commit.

```
address r
for (uint i = 0; i < keys.length; i++){
    r = keys[i] // reuse the variable r instead of creating a new reference every-time
    ....
}
```

- MINOR Recommend emitting event logs for states changing functions. First, it is a good practice using logging for the purpose of history tracing and user behaviors analysis. Second, as the functions declare as `external`, that refer as any users can triggered directly from outside the contract, not necessary go thru by `enter()`.

  – `addOperationKey`
  – `changeAllOperationKeys`
  – `freeze`
  – `unfreeze`
  – `removeBackup`
  – `cancelDelay`
  – `cancelAddBackup`
  – `cancelRemoveBackup`
  – `approveProposal`
  – ✓ MyKey The code is updated and reflected in the latest commit.

- INFO `findBackup` Recommend checking the given `_account` is not an zero address.

  – ✓ MyKey The code is updated and reflected in the latest commit.

AccountStorage.sol

- INFO `setKeyStatus()`: Recommend adding `require()` to ensure `_status` is `0` or `1`.
- INFO `setBackup()`: Recommend adding `require()` to ensure following
  - `_backup` is a non zero address
  - `_effective` should be greater than `now`
  - `_expiry` is later than `now`
  - `_effective` is not later than `_expiry`
- INFO `setBackupExpiryDate()`: Recommend adding `require()` to ensure `_expiry` is later than `now`
- INFO `setDelayData()`: Recommend adding `require()` to ensure
  - `_hash` is a non zero address
  - `_dueTime` is later than `now`

AccountProxy.sol

- INFO Recommend defining the visibility level for variable `implementation` implicitly regarding to the best practice guide

DualsigsLogic.sol

- INFO Recommend changing `isActionWithDualSigs()` from a function to a modifier.
  - ✓ MyKey The `isActionWithDualSigs` is renamed to `allowDualSigsActionOnly` with modifier decorator
- INFO Recommend changing `isFastAction()` from a function to a modifier.
- MINOR `addBackup()` Consider using SafeMath library for adding `now` + getDelayTime to prevent the issue cause by integer underflow or overflow
  - ✓ MyKey The `getDelayTime()` is removed, only (7, 14, 21) days are valid delayed time on main-net.

Owned.sol

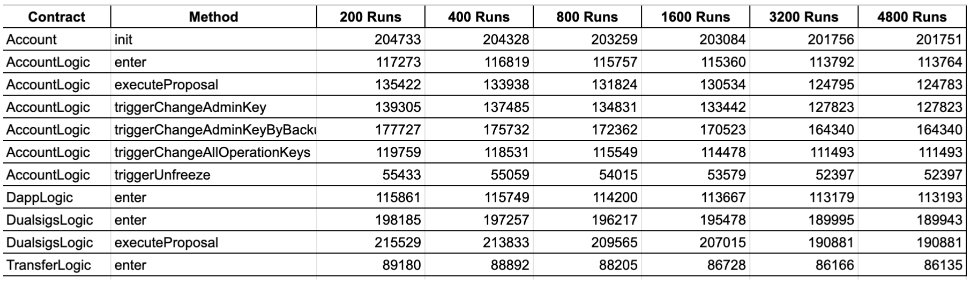
- INFO Given `constructor()` not taking any input parameter, consider keeping the function as `internal`.
- INFO Recommend to record the previous owner address in the event `OwnerChanged` for better tracing context. - i.e: `event OwnerChanged(address indexed previousOwner, address indexed _newOwner);`
  - ✓ MyKey The code is updated and reflected in the latest commit.
- INFO Highly recommend using pull-over-push pattern for ownership transfer, openzepplin's `Ownable` contract, which is a good reference for consideration.

LogicManager.sol

- INFO Recommend changing `if (authorized[_logic] != _value)` in `updateLogic()` to be `require(authorized[_logic] != p.value)` in `triggerUpdateLogic()` before calling `updateLogic()`.
- INFO Recommend `submitUpdate` using SafeMath for `now` + pendingTime for preventing the arithmetic vulnerability

Gas Consumption

The gas consumption is based on localhost environment with optimizer mode and runs with 200, 400, 800, 1600, 3200, and 4000 times



Contract	Method	200 Runs	400 Runs	800 Runs	1600 Runs	3200 Runs	4800 Runs
Account	init	204733	204328	203259	203084	201756	201751
AccountLogic	enter	117273	116819	115757	115360	113792	113764
AccountLogic	executeProposal	135422	133938	131824	130534	124795	124783
AccountLogic	triggerChangeAdminKey	139305	137485	134831	133442	127823	127823
AccountLogic	triggerChangeAdminKeyByBacku	177727	175732	172362	170523	164340	164340
AccountLogic	triggerChangeAllOperationKeys	119759	118531	115549	114478	111493	111493
AccountLogic	triggerUnfreeze	55433	55059	54015	53579	52397	52397
DappLogic	enter	115861	115749	114200	113667	113179	113193
DualsigsLogic	enter	198185	197257	196217	195478	189995	189943
DualsigsLogic	executeProposal	215529	213833	209565	207015	190881	190881
TransferLogic	enter	89180	88892	88205	86728	86166	86135

Best practice

Smart contract development requires a particular engineering mindset. A failure in the initial construction can be catastrophic, and changing the project after the fact can be exceedingly difficult.
To ensure success and to avoid the challenges above smart contracts should here to best practices at their conception. Below, we summarized a checklist of key points & vulnerability vectors that help to indicate a high overall quality of the current MyKey project. (✓ indicates satisfaction; × indicates unsatisfaction; – indicates inapplicable)

General

Overall, smart contract coding practice baseline such as environment setting, compiler version, testing, logging, and code layout.
Compiling

✓ Correct environment settings, e.g. compiler version, test framework

✓ No compiler warnings

Logging

✓ Provide error message along with `assert` & `require`

✓ Use events to monitor contract activities

Code Layout

✓ According to Solidity Tutorial, Layout contract elements should following below order:

1. Pragma statements
2. Import statements
3. Interfaces
4. Libraries
5. Contracts

× Each contract, library or interface should following below order:

1. Type declarations
2. State variables
3. Events
4. Functions

× According to Solidity Tutorial, functions should be grouped according to their visibility and ordered:

1. constructor
2. fallback function (if exists)
3. external
4. public
5. internal
6. private

Arithmetic Vulnerability

EVM specifies fixed-size data types for integers, in which means that has only a certain range of numbers it can store or represent.
Two's Complement / Integer underflow / overflow

✓ Use Math library as SafeMath for all arithmetic operations to handle integer overflow and underflow

Floating Points and Precision

– Correct handling the right precision when dealing ratios and rates

Access & Privilege Control Vulnerability

Authorization of end-user and administrator and his/her assessment rights
Circuit Breaker

✓ Provide pause functionality for control and emergency handling

Restriction

✓ Provide proper access control for functions

- ✓ Establish rate limiter for certain operations
- ✓ Restrict access to sensitive functions
- ✓ Restrict permission to contract destruction
- ✓ Establish speed bumps slow down some sensitive actions, any malicious actions occur, there is time to recover.

DoS Vulnerability

A type of attacks that make the contract inoperable with certain period of time or permanently.
Unexpected Revert

- ✓ Use favor pull over push pattern for handling unexpected revert

Block Gas Limit

- – Use favor pull over push pattern for handling gas spent exceeds its limit on Contract via unbounded operations
- ✓ Use favor pull over push pattern for handling gas spent exceeds its limit on the network via block stuffing

Miner Manipulation Vulnerability

BlockNumber Dependence

- – Understand the security risk level and trade-off of using `block.number` as one of core factors in the contract. Be aware that `block.number` can not be manipulated by the miner, but can lead to large than expected time differences. With assumptions of an Ethereum block confirmation takes 13 seconds. However, the average block time is between 13 15 seconds. During the difficulty bomb stage or hard/soft fork upgrade of the network, `block.number` to a time is dangerous and inaccurate as expected.

Timestamp Dependence

- ✓ Understand the security risk level and trade-off of using `block.timestamp` or alias `now` as one of core factors in the contract.
- ✓ Correct use of 15-second rule to minimize the impact caused by timestamp variance

Transaction Ordering Or Front-Running

- – Understand the security risk level and the `gasPrice` rule in this vulnerability
- – Correct placing an upper bound on the `gasPrice` for preventing the users taking the benefit of transaction ordering

External Referencing Vulnerability

External calls may execute malicious code in that contract or any other contract that it depends upon. As such, every external call should be treated as a potential security risk

- ✓ Correct using the pull over push favor for external calls to reduce reduces the chance of problems with the gas limit.

Avoid state changes after external calls

- ✓ Correct using checks-effects-interactions pattern to minimize the state changes after external contract or call referencing.

Handle errors in external calls

- ✓ Correct handling errors in any external contract or call referencing by checking its return value

Race Conditions Vulnerability

A type of vulnerability caused by calling external contracts that attacker can take over the control flow, and make changes to the data that the calling function wasn't expecting.

- Type of race conditions:
  - Reentrancy
    A state variable is changed after a contract uses `call.value()()`.
  - Cross-function Race Conditions
    An attacker may also be able to do a similar attack using two different functions that share the same state

- ✓ Avoid using `call.value()()`, instead use `send()`, `transfer()` that consumes 2300 gas. This will prevent any external code from being executed continuously

- ✓ Finish all internal work before calling the external function for unavoidable external call.

Low-level Call Vulnerability

The low-level function or opcodes are very useful and danger as for allowing the Libraries implementation and modularized code. However it opens up the doors to vulnerabilities as essentially your contract is allowing anyone to do whatever they want with their state Code Injection by delegatecall

- ✓ Ensure the libraries implementation is stateless and non-self-destructable

Visibility Vulnerability

Solidity functions have 4 difference visibility 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.

- ✓ Specify the visibility of all functions in a contract, even if they are intentionally public

Incorrect Interface Vulnerability

A contract interface defines functions with a different type signature than the implementation, causing two different method id's to be created. As a result, when the interface is called, the fallback method will be executed.

- ✓ Ensure the defined function signatures are match with the contract interface and implementation

Bad Randomness Vulnerability

Pseudo random number generation is not supported by Solidity as default, which it is an unsafe operation.

- ✓ Avoid using randomness for block variables, there may be a chance manipulated by the miners

Documentation

- ✓ Provide project README and execution guidance
- ✓ Provide inline comment for complex functions intention
- ✓ Provide instruction to initialize and execute the test files

Testing

- ✓ Provide migration scripts for continuously contracts deployment to the Ethereum network
- ✓ Provide test scripts and coverage for potential scenarios

Overall we found the smart contracts to follow good practices. With the final update of source code and delivery of the audit report, we conclude that the contract is structurally sound and not vulnerable to any classically known anti-patterns or security issues. The audit report itself is not necessarily a guarantee of correctness or trustworthiness, and we always recommend to seek multiple opinions, keep improving the codebase, and more test coverage and sandbox deployments before the main-net release.

Static Analysis Results

INSECURE_COMPILER_VERSION

Line 1 in File AccountStorage.sol

```
1 pragma solidity ^0.5.4;
```

ⓘ Only these compiler versions are safe to compile your code: 0.5.10

TIMESTAMP_DEPENDENCY

Line 218 in File AccountStorage.sol

```
218             backupData[address(_account)][index] = BackupAccount(_backup, now, uint256
                    (-1));
```

❗ ”now” can be influenced by miners to some degree

INSECURE_COMPILER_VERSION

Line 1 in File AccountProxy.sol

```
1 pragma solidity ^0.5.4;
```

ⓘ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File AccountCreator.sol

```
1 pragma solidity ^0.5.4;
```

ⓘ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File Account.sol

```
1 pragma solidity ^0.5.4;
```

ⓘ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File LogicManager.sol

```
1 pragma solidity ^0.5.4;
```

ⓘ Only these compiler versions are safe to compile your code: 0.5.10

TIMESTAMP_DEPENDENCY

Line 61 in File LogicManager.sol

```
61         p.dueTime = now + pendingTime;
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 72 in File LogicManager.sol

```
72        require(p.dueTime <= now, "too early to trigger updateLogic");
```

❗ ”now” can be influenced by miners to some degree

INSECURE_COMPILER_VERSION

Line 1 in File Owned.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File MultiOwned.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File SafeMath.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File DualsigsLogic.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

TIMESTAMP_DEPENDENCY

Line 137 in File DualsigsLogic.sol

```
137    accountStorage.setBackup(_account, index, _backup, now + DELAY_CHANGE_BACKUP,
           uint256(-1));
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 151 in File DualsigsLogic.sol

```
151      if ((backup == _backup) && (expiryDate > now)) {
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 156 in File DualsigsLogic.sol

```
156        if ((backup == address(0)) || (expiryDate <= now)) {
```

❗ ”now” can be influenced by miners to some degree

INSECURE_COMPILER_VERSION

Line 1 in File AccountLogic.sol

```
1 pragma solidity ^0.5.4;
```

ⓘ Only these compiler versions are safe to compile your code: 0.5.10

TIMESTAMP_DEPENDENCY

Line 72 in File AccountLogic.sol

```
72      accountStorage.setDelayData(_account, CHANGE_ADMIN_KEY, hash, now +
            DELAY_CHANGE_ADMIN_KEY);
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 82 in File AccountLogic.sol

```
82      require(due <= now, "too early to trigger changeAdminKey");
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 100 in File AccountLogic.sol

```
100     accountStorage.setDelayData(_account, CHANGE_ADMIN_KEY_BY_BACKUP, hash, now +
            DELAY_CHANGE_ADMIN_KEY_BY_BACKUP);
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 110 in File AccountLogic.sol

```
110     require(due <= now, "too early to trigger changeAdminKeyByBackup");
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 147 in File AccountLogic.sol

```
147     accountStorage.setDelayData(_account, CHANGE_ALL_OPERATION_KEYS, hash, now +
            DELAY_CHANGE_OPERATION_KEY);
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 157 in File AccountLogic.sol

```
157     require(due <= now, "too early to trigger changeAllOperationKeys");
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 183 in File AccountLogic.sol

```
183     accountStorage.setDelayData(_account, UNFREEZE, hash, now + DELAY_UNFREEZE_KEY);
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 193 in File AccountLogic.sol

```
193     require(due <= now, "too early to trigger unfreeze");
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 211 in File AccountLogic.sol

```
211     accountStorage.setBackupExpiryDate(_account, index, now + DELAY_CHANGE_BACKUP);
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 244 in File AccountLogic.sol

```
244     require(effectiveDate > now, "already effective");
```

❗ ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 253 in File AccountLogic.sol

```
253     require(expiryDate > now, "already expired");
```

❗ ”now” can be influenced by miners to some degree

INSECURE_COMPILER_VERSION

Line 1 in File DappLogic.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File TransferLogic.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

INSECURE_COMPILER_VERSION

Line 1 in File AccountBaseLogic.sol

```
1 pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

TIMESTAMP_DEPENDENCY

Line 107 in File AccountBaseLogic.sol

```
107         return (_effectiveDate <= now) && (_expiryDate > now);
```

! ”now” can be influenced by miners to some degree

TIMESTAMP_DEPENDENCY

Line 107 in File AccountBaseLogic.sol

```
107         return (_effectiveDate <= now) && (_expiryDate > now);
```

! ”now” can be influenced by miners to some degree

INSECURE_COMPILER_VERSION

Line 1 in File BaseLogic.sol

```
1   pragma solidity ^0.5.4;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

TIMESTAMP_DEPENDENCY

Line 156 in File BaseLogic.sol

```
156         require(SafeMath.div(_nonce, 1000000) <= now + 86400, "nonce too big"); //
                86400=24*3600 seconds
```

! ”now” can be influenced by miners to some degree

INSECURE_COMPILER_VERSION

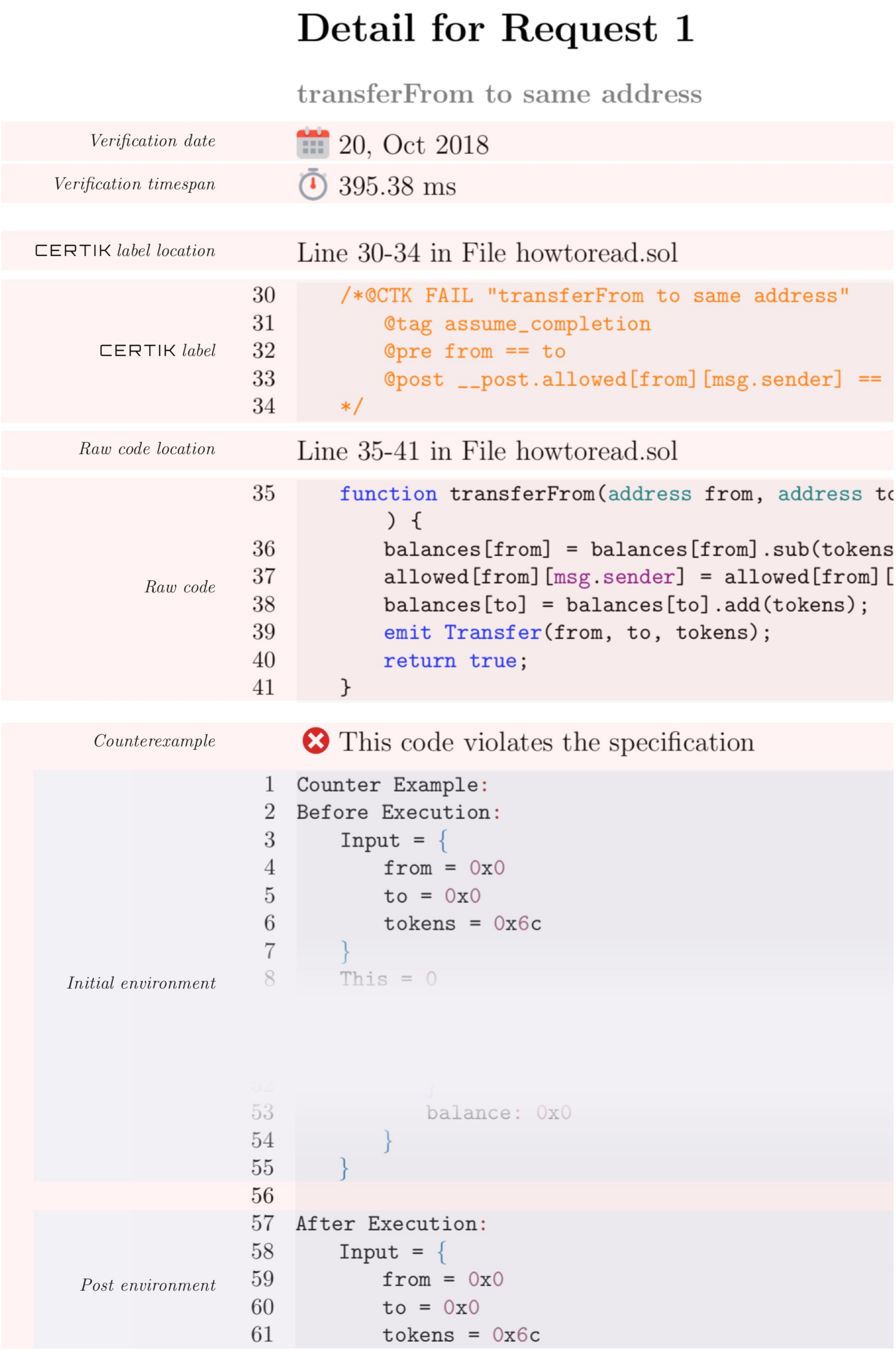
Line 1 in File MyToken.sol

```
1   pragma solidity ^0.5.0;
```

ℹ Only these compiler versions are safe to compile your code: 0.5.10

Formal Verification Results

How to read



Detail for Request 1

transferFrom to same address

Verification date	20, Oct 2018
Verification timespan	395.38 ms
CERTIK *label location*	Line 30-34 in File howtoread.sol

CERTIK *label*

```
30  /*@CTK FAIL "transferFrom to same address"
31      @tag assume_completion
32      @pre from == to
33      @post __post.allowed[from][msg.sender] ==
34  */
```

Raw code location — Line 35-41 in File howtoread.sol

Raw code

```
35  function transferFrom(address from, address t
        ) {
36      balances[from] = balances[from].sub(tokens
37      allowed[from][msg.sender] = allowed[from][
38      balances[to] = balances[to].add(tokens);
39      emit Transfer(from, to, tokens);
40      return true;
41  }
```

Counterexample — ☒ This code violates the specification

Initial environment

```
1   Counter Example:
2   Before Execution:
3       Input = {
4           from = 0x0
5           to = 0x0
6           tokens = 0x6c
7       }
8       This = 0

52              }
53              balance: 0x0
54          }
55      }
56
```

Post environment

```
57  After Execution:
58      Input = {
59          from = 0x0
60          to = 0x0
61          tokens = 0x6c
```

Formal Verification Request 1

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.27 ms

Line 60 in File AccountStorage.sol

```
60      //@CTK NO_ASF
```

Line 61-63 in File AccountStorage.sol

```
61      function getOperationKeyCount(address _account) external view returns(uint256) {
62          return operationKeyCount[_account];
63      }
```

✓ The code meets the specification.

Formal Verification Request 2

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.51 ms

Line 69 in File AccountStorage.sol

```
69      //@CTK NO_ASF
```

Line 70-73 in File AccountStorage.sol

```
70      function getKeyData(address _account, uint256 _index) public view returns(address)
             {
71          KeyItem memory item = keyData[_account][_index];
72          return item.pubKey;
73      }
```

✓ The code meets the specification.

Formal Verification Request 3

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.73 ms

Line 81 in File AccountStorage.sol

```
81      //@CTK NO_ASF
```

Line 82-85 in File AccountStorage.sol

```
82      function getKeyStatus(address _account, uint256 _index) external view returns(
            uint256) {
83          KeyItem memory item = keyData[_account][_index];
84          return item.status;
85      }
```

✓ The code meets the specification.

Formal Verification Request 4

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 7.04 ms

Line 92 in File AccountStorage.sol

```
92    //@CTK NO_ASF
```

Line 93-96 in File AccountStorage.sol

```
93    function getBackupAddress(address _account, uint256 _index) external view returns(
          address) {
94        BackupAccount memory b = backupData[_account][_index];
95        return b.backup;
96    }
```

✓ The code meets the specification.

Formal Verification Request 5

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.54 ms

Line 97 in File AccountStorage.sol

```
97    //@CTK NO_ASF
```

Line 98-101 in File AccountStorage.sol

```
98    function getBackupEffectiveDate(address _account, uint256 _index) external view
          returns(uint256) {
99        BackupAccount memory b = backupData[_account][_index];
100       return b.effectiveDate;
101   }
```

✓ The code meets the specification.

Formal Verification Request 6

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 7.02 ms

Line 102 in File AccountStorage.sol

```
102   //@CTK NO_ASF
```

Line 103-106 in File AccountStorage.sol

```
103   function getBackupExpiryDate(address _account, uint256 _index) external view
          returns(uint256) {
104       BackupAccount memory b = backupData[_account][_index];
105       return b.expiryDate;
106   }
```

✓ The code meets the specification.

Formal Verification Request 7

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 7.09 ms

Line 129 in File AccountStorage.sol

```
129     //@CTK NO_ASF
```

Line 130-133 in File AccountStorage.sol

```
130     function getDelayDataHash(address payable _account, bytes4 _actionId) external
            view returns(bytes32) {
131         DelayItem memory item = delayData[_account][_actionId];
132         return item.hash;
133     }
```

✓ The code meets the specification.

Formal Verification Request 8

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.92 ms

Line 134 in File AccountStorage.sol

```
134     //@CTK NO_ASF
```

Line 135-138 in File AccountStorage.sol

```
135     function getDelayDataDueTime(address payable _account, bytes4 _actionId) external
            view returns(uint256) {
136         DelayItem memory item = delayData[_account][_actionId];
137         return item.dueTime;
138     }
```

✓ The code meets the specification.

Formal Verification Request 9

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 7.47 ms

Line 149 in File AccountStorage.sol

```
149     //@CTK NO_ASF
```

Line 150-153 in File AccountStorage.sol

```
150     function getProposalDataHash(address _client, address _proposer, bytes4 _actionId)
             external view returns(bytes32) {
151         Proposal memory p = proposalData[_client][_proposer][_actionId];
152         return p.hash;
153     }
```

✓ The code meets the specification.

Formal Verification Request 10

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 7.16 ms

Line 154 in File AccountStorage.sol

```
154     //@CTK NO_ASF
```

Line 155-158 in File AccountStorage.sol

```
155     function getProposalDataApproval(address _client, address _proposer, bytes4
            _actionId) external view returns(address[] memory) {
156         Proposal memory p = proposalData[_client][_proposer][_actionId];
157         return p.approval;
158     }
```

✓ The code meets the specification.

Formal Verification Request 11

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 5.94 ms

Line 8 in File AccountProxy.sol

```
8       //@CTK NO_ASF
```

Line 9-11 in File AccountProxy.sol

```
9       constructor(address _implementation) public {
10          implementation = _implementation;
11      }
```

✓ The code meets the specification.

Formal Verification Request 12

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 11.96 ms

Line 19 in File AccountCreator.sol

```
19      //@CTK NO_ASF
```

Line 20-25 in File AccountCreator.sol

```
20      constructor(address _mgr, address _storage, address _accountImpl) public {
21          logicManager = _mgr;
22          accountStorage = _storage;
23          accountImpl = _accountImpl;
24          // logics = _logics;
25      }
```

✓ The code meets the specification.

Formal Verification Request 13

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 38.07 ms

Line 63 in File Account.sol

```
63      //@CTK NO_ASF
```

Line 64-67 in File Account.sol

```
64      function enableStaticCall(address _module, bytes4 _method) external
            allowAuthorizedLogicContractsCallsOnly {
65          enabled[_method] = _module;
66          emit EnabledStaticCall(_module, _method);
67      }
```

✓ The code meets the specification.

Formal Verification Request 14

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.99 ms

Line 49 in File LogicManager.sol

```
49      //@CTK NO_ASF
```

Line 50-52 in File LogicManager.sol

```
50      function isAuthorized(address _logic) external view returns (bool) {
51          return authorized[_logic];
52      }
```

✓ The code meets the specification.

Formal Verification Request 15

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.27 ms

Line 53 in File LogicManager.sol

```
53    //@CTK NO_ASF
```

Line 54-56 in File LogicManager.sol

```
54    function getAuthorizedLogics() external view returns (address[] memory) {
55        return authorizedLogics;
56    }
```

✓ The code meets the specification.

Formal Verification Request 16

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 21.27 ms

Line 57 in File LogicManager.sol

```
57    //@CTK NO_ASF
```

Line 58-63 in File LogicManager.sol

```
58    function submitUpdate(address _logic, bool _value) external onlyOwner {
59        pending storage p = pendingLogics[_logic];
60        p.value = _value;
61        p.dueTime = now + pendingTime;
62        emit UpdateLogicSubmitted(_logic, _value);
63    }
```

✓ The code meets the specification.

Formal Verification Request 17

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 24.37 ms

Line 64 in File LogicManager.sol

```
64    //@CTK NO_ASF
```

Line 65-68 in File LogicManager.sol

```
65    function cancelUpdate(address _logic) external onlyOwner {
66        delete pendingLogics[_logic];
67        emit UpdateLogicCancelled(_logic);
68    }
```

✓ The code meets the specification.

Formal Verification Request 18

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 5.96 ms

Line 22 in File Owned.sol

```
22    //@CTK NO_ASF
```

Line 23-25 in File Owned.sol

```
23    constructor() public {
24        owner = msg.sender;
25    }
```

✓ The code meets the specification.

Formal Verification Request 19

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 29.59 ms

Line 31 in File Owned.sol

```
31     //@CTK NO_ASF
```

Line 32-36 in File Owned.sol

```
32    function changeOwner(address _newOwner) external onlyOwner {
33        require(_newOwner != address(0), "Address must not be null");
34        owner = _newOwner;
35        emit OwnerChanged(_newOwner);
36    }
```

✓ The code meets the specification.

Formal Verification Request 20

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 37.87 ms

Line 15 in File MultiOwned.sol

```
15    //@CTK NO_ASF
```

Line 16-22 in File MultiOwned.sol

```
16    function addOwner(address _owner) external onlyOwner {
17        require(_owner != address(0), "owner must not be 0x0");
18        if(multiOwners[_owner] == false) {
19            multiOwners[_owner] = true;
20            emit OwnerAdded(_owner);
21        }
22    }
```

✓ The code meets the specification.

Formal Verification Request 21

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 30.07 ms

Line 23 in File MultiOwned.sol

```
23    //@CTK NO_ASF
```

Line 24-28 in File MultiOwned.sol

```
24    function removeOwner(address _owner) external onlyOwner {
25        require(multiOwners[_owner] == true, "owner not exist");
26        delete multiOwners[_owner];
27        emit OwnerRemoved(_owner);
28    }
```

✓ The code meets the specification.

Formal Verification Request 22

SafeMath mul

📅 20, Nov 2019
⏱ 240.58 ms

Line 35-40 in File SafeMath.sol

```
35    /*@CTK "SafeMath mul"
36      @post (a > 0) && (((a * b) / a) != b) -> __reverted
37      @post __reverted -> (a > 0) && (((a * b) / a) != b)
38      @post !__reverted -> __return == a * b
39      @post !__reverted == !__has_overflow
40   */
```

Line 41-53 in File SafeMath.sol

```
41    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
42        // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
43        // benefit is lost if 'b' is also tested.
44        // See: https://github.com/OpenZeppelin/openzeppelin-solidity/pull/522
45        if (a == 0) {
46            return 0;
47        }
48
49        uint256 c = a * b;
50        require(c / a == b);
51
52        return c;
53    }
```

✓ The code meets the specification.

Formal Verification Request 23

SafeMath div

📅 20, Nov 2019
⏱ 15.95 ms

Line 58-62 in File SafeMath.sol

```
58    /*@CTK "SafeMath div"
59      @post b != 0 -> !__reverted
60      @post !__reverted -> __return == a / b
61      @post !__reverted -> !__has_overflow
62    */
```

Line 63-69 in File SafeMath.sol

```
63    function div(uint256 a, uint256 b) internal pure returns (uint256) {
64        require(b > 0); // Solidity only automatically asserts when dividing by 0
65        uint256 c = a / b;
66        // assert(a == b * c + a % b); // There is no case in which this doesn't hold
67
68        return c;
69    }
```

✅ The code meets the specification.

Formal Verification Request 24

SafeMath sub

📅 20, Nov 2019
⏱ 14.24 ms

Line 74-78 in File SafeMath.sol

```
74    /*@CTK "SafeMath sub"
75      @post (a < b) == __reverted
76      @post !__reverted -> __return == a - b
77      @post !__reverted -> !__has_overflow
78    */
```

Line 79-84 in File SafeMath.sol

```
79    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
80        require(b <= a);
81        uint256 c = a - b;
82
83        return c;
84    }
```

✅ The code meets the specification.

Formal Verification Request 25

SafeMath add

📅 20, Nov 2019
⏱ 15.66 ms

Line 89-93 in File SafeMath.sol

```
89      /*@CTK "SafeMath add"
90        @post (a + b < a || a + b < b) == __reverted
91        @post !__reverted -> __return == a + b
92        @post !__reverted -> !__has_overflow
93      */
```

Line 94-99 in File SafeMath.sol

```
94      function add(uint256 a, uint256 b) internal pure returns (uint256) {
95          uint256 c = a + b;
96          require(c >= a);
97
98          return c;
99      }
```

✓ The code meets the specification.

Formal Verification Request 26

SafeMath mod

📅 20, Nov 2019
⏱ 14.06 ms

Line 105-109 in File SafeMath.sol

```
105     /*@CTK "SafeMath mod"
106       @post (b == 0) == __reverted
107       @post !__reverted -> __return == a % b
108       @post !__reverted -> !__has_overflow
109     */
```

Line 110-113 in File SafeMath.sol

```
110     function mod(uint256 a, uint256 b) internal pure returns (uint256) {
111         require(b != 0);
112         return a % b;
113     }
```

✓ The code meets the specification.

Formal Verification Request 27

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 70.41 ms

Line 30 in File DualsigsLogic.sol

```
30    //@CTK NO_ASF
```

Line 31-35 in File DualsigsLogic.sol

```
31  constructor(AccountStorage _accountStorage)
32    AccountBaseLogic(_accountStorage)
33    public
34  {
35  }
```

✓ The code meets the specification.

Formal Verification Request 28

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 16.64 ms

Line 38 in File DualsigsLogic.sol

```
38  //@CTK NO_ASF
```

Line 39-41 in File DualsigsLogic.sol

```
39    function initAccount(Account _account) external allowAccountCallsOnly(_account){
40        emit DualsigsLogicInitialised(address(_account));
41    }
```

✓ The code meets the specification.

Formal Verification Request 29

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 12.81 ms

Line 175 in File DualsigsLogic.sol

```
175  //@CTK NO_ASF
```

Line 176-184 in File DualsigsLogic.sol

```
176  function isFastAction(bytes4 _actionId) internal pure returns(bool) {
177    if ((_actionId == CHANGE_ADMIN_KEY_WITHOUT_DELAY) ||
178      (_actionId == CHANGE_ALL_OPERATION_KEYS_WITHOUT_DELAY) ||
179      (_actionId == UNFREEZE_WITHOUT_DELAY))
180    {
181      return true;
182    }
183    return false;
184  }
```

✓ The code meets the specification.

Formal Verification Request 30

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 15.91 ms

Line 187 in File DualsigsLogic.sol

```
187  //@CTK NO_ASF
```

Line 188-196 in File DualsigsLogic.sol

```
188  function getSecondSignerAddress(bytes memory _b) internal pure returns (address _a)
         {
189    require(_b.length >= 68, "data length too short");
190    // solium-disable-next-line security/no-inline-assembly
191    assembly {
192      //68 = 32 + 4 + 32
193      let mask := 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
194      _a := and(mask, mload(add(_b, 68)))
195    }
196  }
```

✅ The code meets the specification.

Formal Verification Request 31

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 14.61 ms

Line 197 in File DualsigsLogic.sol

```
197  //@CTK NO_ASF
```

Line 198-218 in File DualsigsLogic.sol

```
198    function getProposedMethodId(bytes memory _b) internal pure returns (bytes4 _a) {
199    require(_b.length >= 164, "data length too short");
200        // solium-disable-next-line security/no-inline-assembly
201        assembly {
202      /* 'proposeByBoth' data example:
203      0x
204      7548cb94                                                     // method id
205      000000000000000000000000b7055946345ad40f8cca3feb075dfadd9e2641b5 // param 0
206      00000000000000000000000011390e32ccdfb3f85e92b949c72fe482d77838f3 // param 1
207      0000000000000000000000000000000000000000000000000000000000000060 // data length
             including padding
208      0000000000000000000000000000000000000000000000000000000000000044 // true data
             length
209      441d2e50                                                     // method id(
             proposed method: changeAdminKeyWithoutDelay)
210      000000000000000000000000b7055946345ad40f8cca3feb075dfadd9e2641b5 // param 0
211      00000000000000000000000013667a2711960c95fae074f90e0f739bc324d1ed // param 1
212      00000000000000000000000000000000000000000000000000000000     // padding
213      */
214          // the first 32 bytes is the length of the bytes array _b
215     // 32 + 4 + 32 + 32 + 32 + 32 = 164
216           _a := mload(add(_b, 164))
217       }
218   }
```

✓ The code meets the specification.

Formal Verification Request 32

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 67.81 ms

Line 25 in File AccountLogic.sol

```
25  //@CTK NO_ASF
```

Line 26-30 in File AccountLogic.sol

```
26  constructor(AccountStorage _accountStorage)
27    AccountBaseLogic(_accountStorage)
28    public
29  {
30  }
```

✓ The code meets the specification.

Formal Verification Request 33

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 17.09 ms

Line 33 in File AccountLogic.sol

```
33  //@CTK NO_ASF
```

Line 34-36 in File AccountLogic.sol

```
34  function initAccount(Account _account) external allowAccountCallsOnly(_account){
35        emit AccountLogicInitialised(address(_account));
36    }
```

✓ The code meets the specification.

Formal Verification Request 34

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 49.16 ms

Line 295 in File AccountLogic.sol

```
295   //@CTK NO_ASF
```

Line 296-305 in File AccountLogic.sol

```
296  function getKeyIndex(bytes memory _data) internal pure returns (uint256) {
297    uint256 index; //index default value is 0, admin key
298    bytes4 methodId = getMethodId(_data);
299    if (methodId == ADD_OPERATION_KEY) {
300        index = 2; //adding key
301    } else if (methodId == PROPOSE_AS_BACKUP || methodId == APPROVE_PROPOSAL) {
302        index = 4; //assist key
303    }
304    return index;
305  }
```

✓ The code meets the specification.

Formal Verification Request 35

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 27.96 ms

Line 22 in File DappLogic.sol

```
22    //@CTK NO_ASF
```

Line 23-27 in File DappLogic.sol

```
23    constructor(AccountStorage _accountStorage)
24        BaseLogic(_accountStorage)
25        public
26    {
27    }
```

✓ The code meets the specification.

Formal Verification Request 36

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 20.56 ms

Line 30 in File DappLogic.sol

```
30    //@CTK NO_ASF
```

Line 31-33 in File DappLogic.sol

```
31    function initAccount(Account _account) external allowAccountCallsOnly(_account){
32        emit DappLogicInitialised(address(_account));
33    }
```

✓ The code meets the specification.

Formal Verification Request 37

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 23.73 ms

Line 25 in File TransferLogic.sol

```
25    //@CTK NO_ASF
```

Line 26-30 in File TransferLogic.sol

```
26    constructor(AccountStorage _accountStorage)
27    BaseLogic(_accountStorage)
28    public
29  {
30  }
```

✓ The code meets the specification.

Formal Verification Request 38

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 93.21 ms

Line 35 in File TransferLogic.sol

```
35    //@CTK NO_ASF
```

Line 36-39 in File TransferLogic.sol

```
36    function initAccount(Account _account) external allowAccountCallsOnly(_account){
37        _account.enableStaticCall(address(this), ERC721_RECEIVED);
38        emit TransferLogicInitialised(address(_account));
39    }
```

✓ The code meets the specification.

Formal Verification Request 39

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.79 ms

Line 116 in File TransferLogic.sol

```
116   //@CTK NO_ASF
```

Line 117-119 in File TransferLogic.sol

```
117   function onERC721Received(address _operator, address _from, uint256 _tokenId,
          bytes calldata _data) external pure returns (bytes4) {
118       return ERC721_RECEIVED;
119   }
```

✓ The code meets the specification.

Formal Verification Request 40

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 29.84 ms

Line 29 in File AccountBaseLogic.sol

```
29      //@CTK NO_ASF
```

Line 30-34 in File AccountBaseLogic.sol

```
30    constructor(AccountStorage _accountStorage)
31      BaseLogic(_accountStorage)
32      public
33    {
34    }
```

✓ The code meets the specification.

Formal Verification Request 41

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.99 ms

Line 105 in File AccountBaseLogic.sol

```
105      //@CTK NO_ASF
```

Line 106-108 in File AccountBaseLogic.sol

```
106      function isEffectiveBackup(uint256 _effectiveDate, uint256 _expiryDate) internal
             view returns(bool) {
107          return (_effectiveDate <= now) && (_expiryDate > now);
108      }
```

✓ The code meets the specification.

Formal Verification Request 42

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 17.57 ms

Line 33 in File BaseLogic.sol

```
33      //@CTK NO_ASF
```

Line 34-36 in File BaseLogic.sol

```
34      function initAccount(Account _account) external allowAccountCallsOnly(_account){
35          emit LogicInitialised(address(_account));
36      }
```

✓ The code meets the specification.

Formal Verification Request 43

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.51 ms

Line 39 in File BaseLogic.sol

```
39      //@CTK NO_ASF
```

Line 40-42 in File BaseLogic.sol

```
40      function getKeyNonce(address _key) external view returns(uint256) {
41          return keyNonce[_key];
42      }
```

✅ The code meets the specification.

Formal Verification Request 44

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 14.55 ms

Line 122 in File BaseLogic.sol

```
122     //@CTK NO_ASF
```

Line 123-134 in File BaseLogic.sol

```
123     function getSignerAddress(bytes memory _b) internal pure returns (address _a) {
124         require(_b.length >= 36, "invalid bytes");
125         // solium-disable-next-line security/no-inline-assembly
126         assembly {
127             let mask := 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
128             _a := and(mask, mload(add(_b, 36)))
129             // b = {length:32}{method sig:4}{address:32}{...}
130             // 36 is the offset of the first parameter of the data, if encoded properly.
131             // 32 bytes for the length of the bytes array, and the first 4 bytes for the function signature.
132             // 32 bytes is the length of the bytes array!!!!
133         }
134     }
```

✅ The code meets the specification.

Formal Verification Request 45

Method will not encounter an assertion failure.

📅 20, Nov 2019
⏱ 6.39 ms

Line 22 in File MyToken.sol

```
    //@CTK NO_ASF
```

Line 23-25 in File MyToken.sol

```
  function name() public view returns (string memory) {
      return _name;
  }
```

✓ The code meets the specification.

Formal Verification Request 46

Method will not encounter an assertion failure.

20, Nov 2019
6.11 ms

Line 31 in File MyToken.sol

```
    //@CTK NO_ASF
```

Line 32-34 in File MyToken.sol

```
  function symbol() public view returns (string memory) {
      return _symbol;
  }
```

✓ The code meets the specification.

Formal Verification Request 47

Method will not encounter an assertion failure.

20, Nov 2019
5.62 ms

Line 48 in File MyToken.sol

```
    //@CTK NO_ASF
```

Line 49-51 in File MyToken.sol

```
  function decimals() public view returns (uint8) {
      return _decimals;
  }
```

✓ The code meets the specification.

Source Code with CertiK Labels

File AccountStorage.sol

```
pragma solidity ^0.5.4;

import "./Account.sol";
import "./LogicManager.sol";


contract AccountStorage {

    modifier allowAccountCallsOnly(Account _account) {
        require(msg.sender == address(_account), "caller must be account");
        _;
    }

    modifier allowAuthorizedLogicContractsCallsOnly(address payable _account) {
        require(LogicManager(Account(_account).manager()).isAuthorized(msg.sender), "not an authorized logic");
        _;
    }

    struct KeyItem {
        address pubKey;
        uint256 status;
    }

    struct BackupAccount {
        address backup;
        uint256 effectiveDate;//means not effective until this timestamp
        uint256 expiryDate;//means effective until this timestamp
    }

    struct DelayItem {
        bytes32 hash;
        uint256 dueTime;
    }

    struct Proposal {
        bytes32 hash;
        address[] approval;
    }

    // account => quantity of operation keys (index >= 1)
    mapping (address => uint256) operationKeyCount;

    // account => index => KeyItem
    mapping (address => mapping(uint256 => KeyItem)) keyData;

    // account => index => backup account
    mapping (address => mapping(uint256 => BackupAccount)) backupData;

    /* account => actionId => DelayItem

       delayData applies to these 4 actions:
       changeAdminKey, changeAllOperationKeys, unfreeze, changeAdminKeyByBackup
    */
    mapping (address => mapping(bytes4 => DelayItem)) delayData;

    // client account => proposer account => proposed actionId => Proposal
    mapping (address => mapping(address => mapping(bytes4 => Proposal))) proposalData;

    // *************** keyCount ********************** //
    //@CTK NO_ASF
    function getOperationKeyCount(address _account) external view returns(uint256) {
        return operationKeyCount[_account];
    }
    function increaseKeyCount(address payable _account) external
        allowAuthorizedLogicContractsCallsOnly(_account) {
        operationKeyCount[_account] = operationKeyCount[_account] + 1;
    }

    // *************** keyData ********************** //
    //@CTK NO_ASF
    function getKeyData(address _account, uint256 _index) public view returns(address)
         {
        KeyItem memory item = keyData[_account][_index];
        return item.pubKey;
    }
    function setKeyData(address payable _account, uint256 _index, address _key)
        external allowAuthorizedLogicContractsCallsOnly(_account) {
        require(_key != address(0), "invalid _key value");
        KeyItem storage item = keyData[_account][_index];
        item.pubKey = _key;
    }

    // *************** keyStatus ********************** //
    //@CTK NO_ASF
    function getKeyStatus(address _account, uint256 _index) external view returns(
        uint256) {
        KeyItem memory item = keyData[_account][_index];
        return item.status;
    }
    function setKeyStatus(address payable _account, uint256 _index, uint256 _status)
        external allowAuthorizedLogicContractsCallsOnly(_account) {
        KeyItem storage item = keyData[_account][_index];
        item.status = _status;
    }

    // *************** backupData ********************** //
    //@CTK NO_ASF
    function getBackupAddress(address _account, uint256 _index) external view returns(
        address) {
        BackupAccount memory b = backupData[_account][_index];
        return b.backup;
    }
    //@CTK NO_ASF
    function getBackupEffectiveDate(address _account, uint256 _index) external view
        returns(uint256) {
        BackupAccount memory b = backupData[_account][_index];
        return b.effectiveDate;
    }
    //@CTK NO_ASF
    function getBackupExpiryDate(address _account, uint256 _index) external view
        returns(uint256) {
```

```
        BackupAccount memory b = backupData[_account][_index];
        return b.expiryDate;
    }
    function setBackup(address payable _account, uint256 _index, address _backup, uint256 _effective, uint256 _expiry)
        external
        allowAuthorizedLogicContractsCallsOnly(_account)
    {
        BackupAccount storage b = backupData[_account][_index];
        b.backup = _backup;
        b.effectiveDate = _effective;
        b.expiryDate = _expiry;
    }
    function setBackupExpiryDate(address payable _account, uint256 _index, uint256 _expiry)
        external
        allowAuthorizedLogicContractsCallsOnly(_account)
    {
        BackupAccount storage b = backupData[_account][_index];
        b.expiryDate = _expiry;
    }

    function clearBackupData(address payable _account, uint256 _index) external allowAuthorizedLogicContractsCallsOnly(_account) {
        delete backupData[_account][_index];
    }

    // *************** delayData ********************** //
    //@CTK NO_ASF
    function getDelayDataHash(address payable _account, bytes4 _actionId) external view returns(bytes32) {
        DelayItem memory item = delayData[_account][_actionId];
        return item.hash;
    }
    //@CTK NO_ASF
    function getDelayDataDueTime(address payable _account, bytes4 _actionId) external view returns(uint256) {
        DelayItem memory item = delayData[_account][_actionId];
        return item.dueTime;
    }
    function setDelayData(address payable _account, bytes4 _actionId, bytes32 _hash, uint256 _dueTime) external allowAuthorizedLogicContractsCallsOnly(_account) {
        DelayItem storage item = delayData[_account][_actionId];
        item.hash = _hash;
        item.dueTime = _dueTime;
    }
    function clearDelayData(address payable _account, bytes4 _actionId) external allowAuthorizedLogicContractsCallsOnly(_account) {
        delete delayData[_account][_actionId];
    }

    // *************** proposalData ********************** //
    //@CTK NO_ASF
    function getProposalDataHash(address _client, address _proposer, bytes4 _actionId) external view returns(bytes32) {
        Proposal memory p = proposalData[_client][_proposer][_actionId];
        return p.hash;
    }
    //@CTK NO_ASF
    function getProposalDataApproval(address _client, address _proposer, bytes4 _actionId) external view returns(address[] memory) {
        Proposal memory p = proposalData[_client][_proposer][_actionId];
        return p.approval;
    }
    function setProposalData(address payable _client, address _proposer, bytes4 _actionId, bytes32 _hash, address _approvedBackup)
        external
        allowAuthorizedLogicContractsCallsOnly(_client)
    {
        Proposal storage p = proposalData[_client][_proposer][_actionId];
        if (p.hash > 0) {
            if (p.hash == _hash) {
                for (uint256 i = 0; i < p.approval.length; i++) {
                    require(p.approval[i] != _approvedBackup, "backup already exists");
                }
                p.approval.push(_approvedBackup);
            } else {
                p.hash = _hash;
                p.approval.length = 0;
            }
        } else {
            p.hash = _hash;
            p.approval.push(_approvedBackup);
        }
    }
    function clearProposalData(address payable _client, address _proposer, bytes4 _actionId) external allowAuthorizedLogicContractsCallsOnly(_client) {
        delete proposalData[_client][_proposer][_actionId];
    }


    // *************** init ********************** //
    function initAccount(Account _account, address[] calldata _keys, address[] calldata _backups)
        external
        allowAccountCallsOnly(_account)
    {
        require(getKeyData(address(_account), 0) == address(0), "AccountStorage: account already initialized!");
        require(_keys.length > 0, "empty keys array");

        operationKeyCount[address(_account)] = _keys.length - 1;

        for (uint256 index = 0; index < _keys.length; index++) {
            address _key = _keys[index];
            require(_key != address(0), "_key cannot be 0x0");
            KeyItem storage item = keyData[address(_account)][index];
            item.pubKey = _key;
            item.status = 0;
        }

        // avoid backup duplication if _backups.length > 1
        // normally won't check duplication, in most cases only one initial backup when initialization
        if (_backups.length > 1) {
            address[] memory bkps = _backups;
            for (uint256 i = 0; i < _backups.length; i++) {
                for (uint256 j = 0; j < i; j++) {
                    require(bkps[j] != _backups[i], "duplicate backup");
                }
            }
        }

        for (uint256 index = 0; index < _backups.length; index++) {
            address _backup = _backups[index];
            require(_backup != address(0), "backup cannot be 0x0");
            require(_backup != address(_account), "cannot be backup of oneself");

            backupData[address(_account)][index] = BackupAccount(_backup, now, uint256(-1));
        }
    }
}
```

File AccountProxy.sol

```
pragma solidity ^0.5.4;

contract AccountProxy {

    address implementation;

    event Received(uint indexed value, address indexed sender, bytes data);
    //@CTK NO_ASF
    constructor(address _implementation) public {
        implementation = _implementation;
    }
    function() external payable {

        if(msg.data.length == 0 && msg.value > 0) {
            emit Received(msg.value, msg.sender, msg.data);
        }
        else {
            // solium-disable-next-line security/no-inline-assembly
            assembly {
                let target := sload(0)
                calldatacopy(0, 0, calldatasize())
                let result := delegatecall(gas, target, 0, calldatasize(), 0, 0)
                returndatacopy(0, 0, returndatasize())
                switch result
                case 0 {revert(0, returndatasize())}
                default {return (0, returndatasize())}
            }
        }
    }
}
```

File AccountCreator.sol

```
pragma solidity ^0.5.4;

import "./utils/MultiOwned.sol";
import "./Account.sol";
import "./AccountProxy.sol";

contract AccountCreator is MultiOwned {

    address public logicManager;
    address public accountStorage;
    address public accountImpl;
    // address[] public logics;

    // *************** Events *************************** //
    event AccountCreated(address indexed wallet, address[] keys, address[] backups);
    event Closed(address indexed sender);

    // *************** Constructor ********************** //
    //@CTK NO_ASF
    constructor(address _mgr, address _storage, address _accountImpl) public {
        logicManager = _mgr;
        accountStorage = _storage;
        accountImpl = _accountImpl;
        // logics = _logics;
    }

    // *************** External Functions ******************** //
    function createAccount(address[] calldata _keys, address[] calldata _backups)
        external onlyMultiOwners {
        AccountProxy accountProxy = new AccountProxy(accountImpl);
        Account(address(accountProxy)).init(logicManager, accountStorage, LogicManager(
            logicManager).getAuthorizedLogics(), _keys, _backups);

        emit AccountCreated(address(accountProxy), _keys, _backups);
    }

    // *************** Suicide ******************** //
    function close() external onlyMultiOwners {
        selfdestruct(msg.sender);
        emit Closed(msg.sender);
    }
}
```

File Account.sol

```
pragma solidity ^0.5.4;

import "./LogicManager.sol";
import "./logics/base/BaseLogic.sol";
import "./AccountStorage.sol";

contract Account {

    // The implementation of the proxy
    address public implementation;

    // Logic manager
    address public manager;

    // The enabled static calls
    mapping (bytes4 => address) public enabled;

    event EnabledStaticCall(address indexed module, bytes4 indexed method);
    event Invoked(address indexed module, address indexed target, uint indexed value,
        bytes data);
    event Received(uint indexed value, address indexed sender, bytes data);

    event AccountInit(address indexed account);

    modifier allowAuthorizedLogicContractsCallsOnly {
        require(LogicManager(manager).isAuthorized(msg.sender), "not an authorized logic");
        _;
    }
    function init(address _manager, address _accountStorage, address[] calldata _logics, address[] calldata _keys, address[] calldata _backups)
        external
    {
        require(manager == address(0), "Account: account already initialized");
        require(_manager != address(0) && _accountStorage != address(0), "Account: address is null");
        manager = _manager;

        for (uint i = 0; i < _logics.length; i++) {
            address logic = _logics[i];
            require(LogicManager(manager).isAuthorized(logic), "must be authorized logic");

            BaseLogic(logic).initAccount(this);
        }

        AccountStorage(_accountStorage).initAccount(this, _keys, _backups);

        emit AccountInit(address(this));
    }
    function invoke(address _target, uint _value, bytes calldata _data)
        external
        allowAuthorizedLogicContractsCallsOnly
    {
        // solium-disable-next-line security/no-call-value
        (bool success,) = _target.call.value(_value)(_data);
        require(success, "call to target failed");
        emit Invoked(msg.sender, _target, _value, _data);
    }

    /**
    * @dev Enables a static method by specifying the target module to which the call must be delegated.
    * @param _module The target module.
    * @param _method The static method signature.
    */
    //@CTK NO_ASF
    function enableStaticCall(address _module, bytes4 _method) external allowAuthorizedLogicContractsCallsOnly {
        enabled[_method] = _module;
        emit EnabledStaticCall(_module, _method);
    }

     /**
     * @dev This method makes it possible for the wallet to comply to interfaces expecting the wallet to
     * implement specific static methods. It delegates the static call to a target contract if the data corresponds
     * to an enabled method, or logs the call otherwise.
     */
    function() external payable {
        if(msg.data.length > 0) {
            address logic = enabled[msg.sig];
            if(logic == address(0)) {
                emit Received(msg.value, msg.sender, msg.data);
            }
            else {
                require(LogicManager(manager).isAuthorized(logic), "must be an authorized logic for static call");
                // solium-disable-next-line security/no-inline-assembly
                assembly {
                    calldatacopy(0, 0, calldatasize())
                    let result := staticcall(gas, logic, 0, calldatasize(), 0, 0)
                    returndatacopy(0, 0, returndatasize())
                    switch result
                    case 0 {revert(0, returndatasize())}
                    default {return (0, returndatasize())}
                }
            }
        }
    }
}
```

File LogicManager.sol

```
pragma solidity ^0.5.4;

import "./utils/Owned.sol";

contract LogicManager is Owned {

    event UpdateLogicSubmitted(address indexed logic, bool value);
    event UpdateLogicCancelled(address indexed logic);
    event UpdateLogicDone(address indexed logic, bool value);

    struct pending {
        bool value;
        uint dueTime;
    }

    // The authorized logic modules
    mapping (address => bool) public authorized;

    /*
    array
    index 0: AccountLogic address
         1: TransferLogic address
         2: DualsigsLogic address
         3: DappLogic address
         4: ...
     */
    address[] public authorizedLogics;

    // updated logics and their due time of becoming effective
    mapping (address => pending) public pendingLogics;

    // pending time before updated logics take effect
    uint public pendingTime;

    // how many authorized logics
    uint public logicCount;
    constructor(address[] memory _initialLogics, uint256 _pendingTime) public
    {
        for (uint i = 0; i < _initialLogics.length; i++) {
            address logic = _initialLogics[i];
            authorized[logic] = true;
            logicCount += 1;
        }
        authorizedLogics = _initialLogics;

        // pendingTime: 4 days for mainnet, 4 minutes for ropsten testnet
        pendingTime = _pendingTime;
    }
    //@CTK NO_ASF
    function isAuthorized(address _logic) external view returns (bool) {
        return authorized[_logic];
    }
    //@CTK NO_ASF
    function getAuthorizedLogics() external view returns (address[] memory) {
        return authorizedLogics;
    }
    //@CTK NO_ASF
    function submitUpdate(address _logic, bool _value) external onlyOwner {
        pending storage p = pendingLogics[_logic];
        p.value = _value;
        p.dueTime = now + pendingTime;
        emit UpdateLogicSubmitted(_logic, _value);
    }
    //@CTK NO_ASF
    function cancelUpdate(address _logic) external onlyOwner {
        delete pendingLogics[_logic];
        emit UpdateLogicCancelled(_logic);
    }
    function triggerUpdateLogic(address _logic) external {
        pending memory p = pendingLogics[_logic];
        require(p.dueTime > 0, "pending logic not found");
        require(p.dueTime <= now, "too early to trigger updateLogic");
        updateLogic(_logic, p.value);
        delete pendingLogics[_logic];
    }
    function updateLogic(address _logic, bool _value) internal {
        if (authorized[_logic] != _value) {
            if(_value) {
                logicCount += 1;
                authorized[_logic] = true;
                authorizedLogics.push(_logic);
            }
            else {
                logicCount -= 1;
                require(logicCount > 0, "must have at least one logic module");
                delete authorized[_logic];
                removeLogic(_logic);
            }
            emit UpdateLogicDone(_logic, _value);
        }
    }
    function removeLogic(address _logic) internal {
        uint len = authorizedLogics.length;
        address lastLogic = authorizedLogics[len - 1];
        if (_logic != lastLogic) {
            for (uint i = 0; i < len; i++) {
                if (_logic == authorizedLogics[i]) {
                    authorizedLogics[i] = lastLogic;
                    break;
                }
            }
        }
        authorizedLogics.length--;
    }
}
```

File utils/Owned.sol

```
pragma solidity ^0.5.4;

/**
 * @title Owned
 * @dev Basic contract to define an owner.
 * @author Julien Niset - <julien@argent.im>
 */
contract Owned {

    // The owner
    address public owner;

    event OwnerChanged(address indexed _newOwner);

    /**
     * @dev Throws if the sender is not the owner.
     */
    modifier onlyOwner {
        require(msg.sender == owner, "Must be owner");
        _;
    }
    //@CTK NO_ASF
    constructor() public {
        owner = msg.sender;
    }

    /**
     * @dev Lets the owner transfer ownership of the contract to a new owner.
     * @param _newOwner The new owner.
     */
     //@CTK NO_ASF
    function changeOwner(address _newOwner) external onlyOwner {
        require(_newOwner != address(0), "Address must not be null");
        owner = _newOwner;
        emit OwnerChanged(_newOwner);
    }
}
```

File utils/MultiOwned.sol

```
pragma solidity ^0.5.4;

import "./Owned.sol";
```

```

contract MultiOwned is Owned {
    mapping (address => bool) public multiOwners;

    modifier onlyMultiOwners {
        require(multiOwners[msg.sender] == true, "must be one of owners");
        _;
    }

    event OwnerAdded(address indexed _owner);
    event OwnerRemoved(address indexed _owner);
    //@CTK NO_ASF
    function addOwner(address _owner) external onlyOwner {
        require(_owner != address(0), "owner must not be 0x0");
        if(multiOwners[_owner] == false) {
            multiOwners[_owner] = true;
            emit OwnerAdded(_owner);
        }
    }
    //@CTK NO_ASF
    function removeOwner(address _owner) external onlyOwner {
        require(multiOwners[_owner] == true, "owner not exist");
        delete multiOwners[_owner];
        emit OwnerRemoved(_owner);
    }
}
```

File utils/SafeMath.sol

```
pragma solidity ^0.5.4;

/* The MIT License (MIT)

Copyright (c) 2016 Smart Contract Solutions, Inc.

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,
TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. */

/**
 * @title SafeMath
 * @dev Math operations with safety checks that throw on error
 */
library SafeMath {

    /**
    * @dev Multiplies two numbers, reverts on overflow.
    */
    /*@CTK "SafeMath mul"
      @post (a > 0) && (((a * b) / a) != b) -> __reverted
      @post __reverted -> (a > 0) && (((a * b) / a) != b)
      @post !__reverted -> __return == a * b
      @post !__reverted == !__has_overflow
   */
    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
        // Gas optimization: this is cheaper than requiring 'a' not being zero, but the
        // benefit is lost if 'b' is also tested.
        // See: https://github.com/OpenZeppelin/openzeppelin-solidity/pull/522
        if (a == 0) {
            return 0;
        }

        uint256 c = a * b;
        require(c / a == b);

        return c;
    }

    /**
    * @dev Integer division of two numbers truncating the quotient, reverts on division by zero.
    */
    /*@CTK "SafeMath div"
      @post b != 0 -> !__reverted
      @post !__reverted -> __return == a / b
      @post !__reverted -> !__has_overflow
    */
    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        require(b > 0); // Solidity only automatically asserts when dividing by 0
        uint256 c = a / b;
        // assert(a == b * c + a % b); // There is no case in which this doesn't hold

        return c;
    }

    /**
    * @dev Subtracts two numbers, reverts on overflow (i.e. if subtrahend is greater than minuend).
    */
    /*@CTK "SafeMath sub"
      @post (a < b) == __reverted
      @post !__reverted -> __return == a - b
      @post !__reverted -> !__has_overflow
    */
    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        require(b <= a);
        uint256 c = a - b;

        return c;
    }

    /**
    * @dev Adds two numbers, reverts on overflow.
    */
    /*@CTK "SafeMath add"
      @post (a + b < a || a + b < b) == __reverted
      @post !__reverted -> __return == a + b
      @post !__reverted -> !__has_overflow
    */
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a + b;
        require(c >= a);

        return c;
    }

    /**
    * @dev Divides two numbers and returns the remainder (unsigned integer modulo),
    * reverts when dividing by zero.
    */
    /*@CTK "SafeMath mod"
      @post (b == 0) == __reverted
      @post !__reverted -> __return == a % b
      @post !__reverted -> !__has_overflow
    */
    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        require(b != 0);
        return a % b;
    }

    /**
    * @dev Returns ceil(a / b).
    */
    function ceil(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a / b;
        if(a % b == 0) {
            return c;
        }
        else {
            return c + 1;
        }
    }
}
```

File logics/DualsigsLogic.sol

```
pragma solidity ^0.5.4;

import "./base/AccountBaseLogic.sol";

/**
* @title DualsigsLogic
*/
contract DualsigsLogic is AccountBaseLogic {

  // Equals to bytes4(keccak256("changeAllOperationKeysWithoutDelay(address,address[])"))
  bytes4 private constant CHANGE_ALL_OPERATION_KEYS_WITHOUT_DELAY = 0x02064abc;
  // Equals to bytes4(keccak256("unfreezeWithoutDelay(address)"))
  bytes4 private constant UNFREEZE_WITHOUT_DELAY = 0x69521650;
  // Equals to bytes4(keccak256("addBackup(address,address)"))
```

```
bytes4 private constant ADD_BACKUP = 0x426b7407;
// Equals to bytes4(keccak256("proposeByBoth(address,address,bytes)"))
bytes4 private constant PROPOSE_BY_BOTH = 0x7548cb94;

  event DualsigsLogicInitialised(address indexed account);
  event DualsigsLogicEntered(bytes data, uint256 indexed clientNonce, uint256 backupNonce);

modifier allowDualSigsActionOnly(bytes memory _data) {
  bytes4 methodId = getMethodId(_data);
  require ((methodId == ADD_BACKUP) ||
        (methodId == PROPOSE_BY_BOTH), "wrong entry");
  _;
}

// *************** Constructor ********************** //
//@CTK NO_ASF
constructor(AccountStorage _accountStorage)
  AccountBaseLogic(_accountStorage)
  public
{
}

  // *************** Initialization ********************* //
//@CTK NO_ASF
  function initAccount(Account _account) external allowAccountCallsOnly(_account){
      emit DualsigsLogicInitialised(address(_account));
  }

// *************** action entry ********************** //

  /* DualsigsLogic has 2 actions called from 'enter':
      addBackup, proposeByBoth
*/
function enter(
  bytes calldata _data, bytes calldata _clientSig, bytes calldata _backupSig, uint256 _clientNonce, uint256 _backupNonce
)
  external allowDualSigsActionOnly(_data)
{
      verifyClient(_data, _clientSig, _clientNonce);
      verifyBackup(_data, _backupSig, _backupNonce);

  // solium-disable-next-line security/no-low-level-calls
  (bool success,) = address(this).call(_data);
  require(success, "enterWithDualSigs failed");
  emit DualsigsLogicEntered(_data, _clientNonce, _backupNonce);
}
function verifyClient(bytes memory _data, bytes memory _clientSig, uint256 _clientNonce) internal {
  address client = getSignerAddress(_data);
  //client sign with admin key
  uint256 clientKeyIndex = 0;
  checkKeyStatus(client, clientKeyIndex);
  address signingKey = accountStorage.getKeyData(client, clientKeyIndex);
  if ((getMethodId(_data) == PROPOSE_BY_BOTH) &&
      (getProposedMethodId(_data) == CHANGE_ADMIN_KEY_WITHOUT_DELAY)) {
    // if proposed action is 'changeAdminKeyWithoutDelay', do not check _clientNonce
    verifySig(signingKey, _clientSig, getSignHashWithoutNonce(_data));
  } else {
    checkAndUpdateNonce(signingKey, _clientNonce);
    verifySig(signingKey, _clientSig, getSignHash(_data, _clientNonce));
  }
}
  function verifyBackup(bytes memory _data, bytes memory _backupSig, uint256 _backupNonce) internal {
  address backup = getSecondSignerAddress(_data);
  //backup sign with assist key
  uint256 backupKeyIndex = 4;
  checkKeyStatus(backup, backupKeyIndex);
  verifySig(accountStorage.getKeyData(backup, backupKeyIndex), _backupSig, getSignHash(_data, _backupNonce));
  address signingKey = accountStorage.getKeyData(backup, backupKeyIndex);
  checkAndUpdateNonce(signingKey, _backupNonce);
  verifySig(signingKey, _backupSig, getSignHash(_data, _backupNonce));
}

// *************** change admin key ********************** //

  // called from 'executeProposal'
function changeAdminKeyWithoutDelay(address payable _account, address _pkNew) external allowSelfCallsOnly {
  address pk = accountStorage.getKeyData(_account, 0);
  require(pk != _pkNew, "identical admin key already exists");
  require(_pkNew != address(0), "0x0 is invalid");
  accountStorage.setKeyData(_account, 0, _pkNew);
  //clear any existing related delay data and proposal
  accountStorage.clearDelayData(_account, CHANGE_ADMIN_KEY);
  accountStorage.clearDelayData(_account, CHANGE_ADMIN_KEY_BY_BACKUP);
  accountStorage.clearDelayData(_account, CHANGE_ALL_OPERATION_KEYS);
  accountStorage.clearDelayData(_account, UNFREEZE);
  clearRelatedProposalAfterAdminKeyChanged(_account);
}

// *************** change all operation keys ********************** //

  // called from 'executeProposal'
function changeAllOperationKeysWithoutDelay(address payable _account, address[] calldata _pks) external allowSelfCallsOnly {
  uint256 keyCount = accountStorage.getOperationKeyCount(_account);
  require(_pks.length == keyCount, "invalid number of keys");
  for (uint256 i = 0; i < keyCount; i++) {
    address pk = _pks[i];
    require(pk != address(0), "0x0 is invalid");
    accountStorage.setKeyData(_account, i+1, pk);
    accountStorage.setKeyStatus(_account, i+1, 0);
  }
}

// *************** freeze/unfreeze all operation keys ********************** //

  // called from 'executeProposal'
function unfreezeWithoutDelay(address payable _account) external allowSelfCallsOnly {
  for (uint256 i = 0; i < accountStorage.getOperationKeyCount(_account); i++) {
    if (accountStorage.getKeyStatus(_account, i+1) == 1) {
```

```
   accountStorage.setKeyStatus(_account, i+1, 0);
  }
 }
}

// *************** add backup ********************** //

 // called from ’enter’
function addBackup(address payable _account, address _backup) external allowSelfCallsOnly {
 require(_account != _backup, "cannot be backup of oneself");
 uint256 index = findAvailableSlot(_account, _backup);
 require(index <= MAX_DEFINED_BACKUP_INDEX, "invalid or duplicate or no vacancy");
 accountStorage.setBackup(_account, index, _backup, now + DELAY_CHANGE_BACKUP, uint256(-1));
}

 // return backupData index(0~5), 6 means not found
 // ’available’ means empty or expired
function findAvailableSlot(address _account, address _backup) public view returns(uint) {
 uint index = MAX_DEFINED_BACKUP_INDEX + 1;
 if (_backup == address(0)) {
  return index;
 }
 for (uint256 i = 0; i <= MAX_DEFINED_BACKUP_INDEX; i++) {
     address backup = accountStorage.getBackupAddress(_account, i);
     uint256 expiryDate = accountStorage.getBackupExpiryDate(_account, i);
  // _backup already exists and not expired
  if ((backup == _backup) && (expiryDate > now)) {
   return MAX_DEFINED_BACKUP_INDEX + 1;
  }
  if (index > MAX_DEFINED_BACKUP_INDEX) {
   // zero address or backup expired
   if ((backup == address(0)) || (expiryDate <= now)) {
        index = i;
   }
  }
 }
 return index;
}

// *************** propose, approve, execute and cancel proposal ********************** //

 // called from ’enter’
// proposer is client in the case of ’proposeByBoth’
function proposeByBoth(address payable _client, address _backup, bytes calldata _functionData) external allowSelfCallsOnly {
 bytes4 proposedActionId = getMethodId(_functionData);
 require(isFastAction(proposedActionId), "invalid proposal");
 checkRelation(_client, _backup);
 bytes32 functionHash = keccak256(_functionData);
 accountStorage.setProposalData(_client, _client, proposedActionId, functionHash, _backup);
}
//@CTK NO_ASF
function isFastAction(bytes4 _actionId) internal pure returns(bool) {
    if ((_actionId == CHANGE_ADMIN_KEY_WITHOUT_DELAY) ||
      (_actionId == CHANGE_ALL_OPERATION_KEYS_WITHOUT_DELAY) ||
      (_actionId == UNFREEZE_WITHOUT_DELAY))
    {
      return true;
    }
    return false;
  }

  // *************** internal functions ********************** //
  //@CTK NO_ASF
  function getSecondSignerAddress(bytes memory _b) internal pure returns (address _a) {
    require(_b.length >= 68, "data length too short");
    // solium-disable-next-line security/no-inline-assembly
    assembly {
      //68 = 32 + 4 + 32
      let mask := 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
      _a := and(mask, mload(add(_b, 68)))
    }
  }
  //@CTK NO_ASF
    function getProposedMethodId(bytes memory _b) internal pure returns (bytes4 _a) {
    require(_b.length >= 164, "data length too short");
        // solium-disable-next-line security/no-inline-assembly
        assembly {
      /* 'proposeByBoth' data example:
      0x
      7548cb94                                                     // method id
      000000000000000000000000b7055946345ad40f8cca3feb075dfadd9e2641b5 // param 0
      00000000000000000000000011390e32ccdfb3f85e92b949c72fe482d77838f3 // param 1
      0000000000000000000000000000000000000000000000000000000000000060 // data length including padding
      0000000000000000000000000000000000000000000000000000000000000044 // true data length
      441d2e50                                                     // method id(proposed method: changeAdminKeyWithoutDelay)
      000000000000000000000000b7055946345ad40f8cca3feb075dfadd9e2641b5 // param 0
      00000000000000000000000013667a2711960c95fae074f90e0f739bc324d1ed // param 1
      00000000000000000000000000000000000000000000000000000000     // padding
      */
           // the first 32 bytes is the length of the bytes array _b
      // 32 + 4 + 32 + 32 + 32 + 32 = 164
           _a := mload(add(_b, 164))
        }
    }
    function getSignHashWithoutNonce(bytes memory _data) internal view returns(bytes32) {
        // use EIP 191
        // 0x1900 + this logic address + data
        bytes32 msgHash = keccak256(abi.encodePacked(byte(0x19), byte(0), address(this), _data));
        bytes32 prefixedHash = keccak256(abi.encodePacked(SIGN_HASH_PREFIX, msgHash));
        return prefixedHash;
    }

}
```

File logics/AccountLogic.sol

```
pragma solidity ^0.5.4;

import "./base/AccountBaseLogic.sol";

/**
* @title AccountLogic
*/
contract AccountLogic is AccountBaseLogic {

  // Equals to bytes4(keccak256("addOperationKey(address,address)"))
  bytes4 private constant ADD_OPERATION_KEY = 0x9a7f6101;
  // Equals to bytes4(keccak256("proposeAsBackup(address,address,bytes)"))
  bytes4 private constant PROPOSE_AS_BACKUP = 0xd470470f;
  // Equals to bytes4(keccak256("approveProposal(address,address,address,bytes)"))
  bytes4 private constant APPROVE_PROPOSAL = 0x3713f742;

    event AccountLogicEntered(bytes data, uint256 indexed nonce);
  event AccountLogicInitialised(address indexed account);
  event ChangeAdminKeyTriggered(address indexed account, address pkNew);
  event ChangeAdminKeyByBackupTriggered(address indexed account, address pkNew);
  event ChangeAllOperationKeysTriggered(address indexed account, address[] pks);
  event UnfreezeTriggered(address indexed account);

  // *************** Constructor ********************** //
  //@CTK NO_ASF
  constructor(AccountStorage _accountStorage)
    AccountBaseLogic(_accountStorage)
    public
  {
  }

    // *************** Initialization ********************* //
  //@CTK NO_ASF
  function initAccount(Account _account) external allowAccountCallsOnly(_account){
       emit AccountLogicInitialised(address(_account));
    }

  // *************** action entry ********************** //

    /* AccountLogic has 12 actions called from 'enter':
       changeAdminKey, addOperationKey, changeAllOperationKeys, freeze, unfreeze,
    removeBackup, cancelDelay, cancelAddBackup, cancelRemoveBackup,
    proposeAsBackup, approveProposal, cancelProposal
  */
  function enter(bytes calldata _data, bytes calldata _signature, uint256 _nonce) external {
    require(getMethodId(_data) != CHANGE_ADMIN_KEY_BY_BACKUP, "invalid data");
    address account = getSignerAddress(_data);
    uint256 keyIndex = getKeyIndex(_data);
    checkKeyStatus(account, keyIndex);
    address signingKey = accountStorage.getKeyData(account, keyIndex);
    checkAndUpdateNonce(signingKey, _nonce);
    bytes32 signHash = getSignHash(_data, _nonce);
    verifySig(signingKey, _signature, signHash);

    // solium-disable-next-line security/no-low-level-calls
    (bool success,) = address(this).call(_data);
    require(success, "calling self failed");
    emit AccountLogicEntered(_data, _nonce);
  }

  // *************** change admin key ********************* //

    // called from 'enter'
  function changeAdminKey(address payable _account, address _pkNew) external
      allowSelfCallsOnly {
    require(_pkNew != address(0), "0x0 is invalid");
    address pk = accountStorage.getKeyData(_account, 0);
    require(pk != _pkNew, "identical admin key exists");
    require(accountStorage.getDelayDataHash(_account, CHANGE_ADMIN_KEY) == 0, "delay
        data already exists");
    bytes32 hash = keccak256(abi.encodePacked('changeAdminKey', _account, _pkNew));
    accountStorage.setDelayData(_account, CHANGE_ADMIN_KEY, hash, now +
        DELAY_CHANGE_ADMIN_KEY);
  }

    // called from external
  function triggerChangeAdminKey(address payable _account, address _pkNew) external {
    bytes32 hash = keccak256(abi.encodePacked('changeAdminKey', _account, _pkNew));
    require(hash == accountStorage.getDelayDataHash(_account, CHANGE_ADMIN_KEY), "
        delay hash unmatch");

    uint256 due = accountStorage.getDelayDataDueTime(_account, CHANGE_ADMIN_KEY);
    require(due > 0, "delay data not found");
    require(due <= now, "too early to trigger changeAdminKey");
    accountStorage.setKeyData(_account, 0, _pkNew);
    //clear any existing related delay data and proposal
    accountStorage.clearDelayData(_account, CHANGE_ADMIN_KEY);
    accountStorage.clearDelayData(_account, CHANGE_ADMIN_KEY_BY_BACKUP);
    clearRelatedProposalAfterAdminKeyChanged(_account);
    emit ChangeAdminKeyTriggered(_account, _pkNew);
  }

  // *************** change admin key by backup proposal ********************* //

    // called from 'executeProposal'
  function changeAdminKeyByBackup(address payable _account, address _pkNew) external
      allowSelfCallsOnly {
    require(_pkNew != address(0), "0x0 is invalid");
    address pk = accountStorage.getKeyData(_account, 0);
    require(pk != _pkNew, "identical admin key exists");
    require(accountStorage.getDelayDataHash(_account, CHANGE_ADMIN_KEY_BY_BACKUP) ==
        0, "delay data already exists");
    bytes32 hash = keccak256(abi.encodePacked('changeAdminKeyByBackup', _account,
        _pkNew));
    accountStorage.setDelayData(_account, CHANGE_ADMIN_KEY_BY_BACKUP, hash, now +
        DELAY_CHANGE_ADMIN_KEY_BY_BACKUP);
  }

    // called from external
  function triggerChangeAdminKeyByBackup(address payable _account, address _pkNew)
      external {
    bytes32 hash = keccak256(abi.encodePacked('changeAdminKeyByBackup', _account,
        _pkNew));
    require(hash == accountStorage.getDelayDataHash(_account,
        CHANGE_ADMIN_KEY_BY_BACKUP), "delay hash unmatch");

    uint256 due = accountStorage.getDelayDataDueTime(_account,
        CHANGE_ADMIN_KEY_BY_BACKUP);
    require(due > 0, "delay data not found");
    require(due <= now, "too early to trigger changeAdminKeyByBackup");
    accountStorage.setKeyData(_account, 0, _pkNew);
    //clear any existing related delay data and proposal
    accountStorage.clearDelayData(_account, CHANGE_ADMIN_KEY_BY_BACKUP);
    accountStorage.clearDelayData(_account, CHANGE_ADMIN_KEY);
    clearRelatedProposalAfterAdminKeyChanged(_account);
    emit ChangeAdminKeyByBackupTriggered(_account, _pkNew);
  }

  // *************** add operation key ********************** //

    // called from 'enter'
  function addOperationKey(address payable _account, address _pkNew) external
      allowSelfCallsOnly {
    uint256 index = accountStorage.getOperationKeyCount(_account) + 1;
    require(index > 0, "invalid operation key index");
    // set a limit to prevent unnecessary trouble
    require(index < 20, "index exceeds limit");
    require(_pkNew != address(0), "0x0 is invalid");
    address pk = accountStorage.getKeyData(_account, index);
    require(pk == address(0), "operation key already exists");
    accountStorage.setKeyData(_account, index, _pkNew);
    accountStorage.increaseKeyCount(_account);
  }

  // *************** change all operation keys ********************** //

    // called from 'enter'
  function changeAllOperationKeys(address payable _account, address[] calldata _pks)
      external allowSelfCallsOnly {
    uint256 keyCount = accountStorage.getOperationKeyCount(_account);
    require(_pks.length == keyCount, "invalid number of keys");
    require(accountStorage.getDelayDataHash(_account, CHANGE_ALL_OPERATION_KEYS) == 0,
         "delay data already exists");
    address pk;
    for (uint256 i = 0; i < keyCount; i++) {
      pk = _pks[i];
      require(pk != address(0), "0x0 is invalid");
    }
    bytes32 hash = keccak256(abi.encodePacked('changeAllOperationKeys', _account, _pks
        ));
    accountStorage.setDelayData(_account, CHANGE_ALL_OPERATION_KEYS, hash, now +
        DELAY_CHANGE_OPERATION_KEY);
  }

    // called from external
  function triggerChangeAllOperationKeys(address payable _account, address[] calldata
      _pks) external {
    bytes32 hash = keccak256(abi.encodePacked('changeAllOperationKeys', _account, _pks
        ));
    require(hash == accountStorage.getDelayDataHash(_account,
        CHANGE_ALL_OPERATION_KEYS), "delay hash unmatch");

    uint256 due = accountStorage.getDelayDataDueTime(_account, CHANGE_ALL_OPERATION_KEYS);
    require(due > 0, "delay data not found");
    require(due <= now, "too early to trigger changeAllOperationKeys");
    address pk;
    for (uint256 i = 0; i < accountStorage.getOperationKeyCount(_account); i++) {
      pk = _pks[i];
      accountStorage.setKeyData(_account, i+1, pk);
      accountStorage.setKeyStatus(_account, i+1, 0);
    }
    accountStorage.clearDelayData(_account, CHANGE_ALL_OPERATION_KEYS);
    emit ChangeAllOperationKeysTriggered(_account, _pks);
  }

  // *************** freeze/unfreeze all operation keys ********************** //

    // called from 'enter'
  function freeze(address payable _account) external allowSelfCallsOnly {
    for (uint256 i = 1; i <= accountStorage.getOperationKeyCount(_account); i++) {
      if (accountStorage.getKeyStatus(_account, i) == 0) {
        accountStorage.setKeyStatus(_account, i, 1);
      }
    }
  }

    // called from 'enter'
  function unfreeze(address payable _account) external allowSelfCallsOnly {
    require(accountStorage.getDelayDataHash(_account, UNFREEZE) == 0, "delay data already exists");
    bytes32 hash = keccak256(abi.encodePacked('unfreeze', _account));
    accountStorage.setDelayData(_account, UNFREEZE, hash, now + DELAY_UNFREEZE_KEY);
  }

    // called from external
  function triggerUnfreeze(address payable _account) external {
    bytes32 hash = keccak256(abi.encodePacked('unfreeze', _account));
    require(hash == accountStorage.getDelayDataHash(_account, UNFREEZE), "delay hash unmatch");

    uint256 due = accountStorage.getDelayDataDueTime(_account, UNFREEZE);
    require(due > 0, "delay data not found");
    require(due <= now, "too early to trigger unfreeze");

    for (uint256 i = 1; i <= accountStorage.getOperationKeyCount(_account); i++) {
      if (accountStorage.getKeyStatus(_account, i) == 1) {
        accountStorage.setKeyStatus(_account, i, 0);
      }
    }
    accountStorage.clearDelayData(_account, UNFREEZE);
    emit UnfreezeTriggered(_account);
  }

  // *************** remove backup ********************** //

    // called from 'enter'
  function removeBackup(address payable _account, address _backup) external allowSelfCallsOnly {
    uint256 index = findBackup(_account, _backup);
    require(index <= MAX_DEFINED_BACKUP_INDEX, "backup invalid or not exist");

    accountStorage.setBackupExpiryDate(_account, index, now + DELAY_CHANGE_BACKUP);
  }

    // return backupData index(0˜5), 6 means not found
    // do make sure _backup is not 0x0
  function findBackup(address _account, address _backup) public view returns(uint) {
    uint index = MAX_DEFINED_BACKUP_INDEX + 1;
    if (_backup == address(0)) {
      return index;
    }
    address b;
    for (uint256 i = 0; i <= MAX_DEFINED_BACKUP_INDEX; i++) {
      b = accountStorage.getBackupAddress(_account, i);
      if (b == _backup) {
        index = i;
        break;
      }
    }
    return index;
  }

  // *************** cancel delay action ********************** //

    // called from ’enter’
  function cancelDelay(address payable _account, bytes4 _actionId) external allowSelfCallsOnly {
    accountStorage.clearDelayData(_account, _actionId);
  }

    // called from ’enter’
  function cancelAddBackup(address payable _account, address _backup) external allowSelfCallsOnly {
    uint256 index = findBackup(_account, _backup);
    require(index <= MAX_DEFINED_BACKUP_INDEX, "backup invalid or not exist");
    uint256 effectiveDate = accountStorage.getBackupEffectiveDate(_account, index);
    require(effectiveDate > now, "already effective");
    accountStorage.clearBackupData(_account, index);
  }

    // called from ’enter’
  function cancelRemoveBackup(address payable _account, address _backup) external allowSelfCallsOnly {
    uint256 index = findBackup(_account, _backup);
    require(index <= MAX_DEFINED_BACKUP_INDEX, "backup invalid or not exist");
    uint256 expiryDate = accountStorage.getBackupExpiryDate(_account, index);
    require(expiryDate > now, "already expired");
    accountStorage.setBackupExpiryDate(_account, index, uint256(-1));
  }

  // *************** propose, approve and cancel proposal ********************** //

    // called from ’enter’
  // proposer is backup in the case of ’proposeAsBackup’
  function proposeAsBackup(address _backup, address payable _client, bytes calldata _functionData) external allowSelfCallsOnly {
    bytes4 proposedActionId = getMethodId(_functionData);
    require(proposedActionId == CHANGE_ADMIN_KEY_BY_BACKUP, "invalid proposal by backup");
    checkRelation(_client, _backup);
    bytes32 functionHash = keccak256(_functionData);
    accountStorage.setProposalData(_client, _backup, proposedActionId, functionHash, _backup);
  }

    // called from 'enter'
  function approveProposal(address _backup, address payable _client, address _proposer, bytes calldata _functionData) external allowSelfCallsOnly {
    bytes32 functionHash = keccak256(_functionData);
    require(functionHash != 0, "invalid hash");
    checkRelation(_client, _backup);
    bytes4 proposedActionId = getMethodId(_functionData);
    bytes32 hash = accountStorage.getProposalDataHash(_client, _proposer, proposedActionId);
    require(hash == functionHash, "proposal unmatch");
    accountStorage.setProposalData(_client, _proposer, proposedActionId, functionHash, _backup);
  }

    // called from 'enter'
  function cancelProposal(address payable _client, address _proposer, bytes4 _proposedActionId) external allowSelfCallsOnly {
    require(_client != _proposer, "cannot cancel dual signed proposal");
    accountStorage.clearProposalData(_client, _proposer, _proposedActionId);
  }

  // *************** internal functions ********************** //

    /*
    index 0: admin key
          1: asset(transfer)
          2: adding
          3: reserved(dapp)
          4: assist
     */
   //@CTK NO_ASF
  function getKeyIndex(bytes memory _data) internal pure returns (uint256) {
    uint256 index; //index default value is 0, admin key
    bytes4 methodId = getMethodId(_data);
    if (methodId == ADD_OPERATION_KEY) {
        index = 2; //adding key
    } else if (methodId == PROPOSE_AS_BACKUP || methodId == APPROVE_PROPOSAL) {
        index = 4; //assist key
    }
    return index;
  }

}
```

File logics/DappLogic.sol

```
pragma solidity ^0.5.4;

import "./base/BaseLogic.sol";

contract DappLogic is BaseLogic {

    /*
    index 0: admin key
          1: asset(transfer)
          2: adding
          3: reserved(dapp)
          4: assist
     */
    uint constant internal DAPP_KEY_INDEX = 3;

    // *************** Events *************************** //

    event DappLogicInitialised(address indexed account);
    event DappLogicEntered(bytes data, uint256 indexed nonce);

    // *************** Constructor ********************** //
    //@CTK NO_ASF
    constructor(AccountStorage _accountStorage)
        BaseLogic(_accountStorage)
        public
    {
    }

    // *************** Initialization ********************* //
    //@CTK NO_ASF
    function initAccount(Account _account) external allowAccountCallsOnly(_account){
        emit DappLogicInitialised(address(_account));
    }

    // *************** action entry ********************* //
    function enter(bytes calldata _data, bytes calldata _signature, uint256 _nonce) external {
        address account = getSignerAddress(_data);
        checkKeyStatus(account, DAPP_KEY_INDEX);

        address dappKey = accountStorage.getKeyData(account, DAPP_KEY_INDEX);
        heckAndUpdateNonce(dappKey, _nonce);
        bytes32 signHash = getSignHash(_data, _nonce);
        verifySig(dappKey, _signature, signHash);

        // solium-disable-next-line security/no-low-level-calls
        (bool success,) = address(this).call(_data);
        require(success, "calling self failed");
        emit DappLogicEntered(_data, _nonce);
    }

    // *************** call Dapp ******************** //

    // called from 'enter'
    // call other contract from base account
    function callContract(address payable _account, address payable _target, uint256 _value, bytes calldata _methodData) external allowSelfCallsOnly {
        Account(_account).invoke(_target, _value, _methodData);
    }

}
```

File logics/TransferLogic.sol

```
pragma solidity ^0.5.4;

import "./base/BaseLogic.sol";

contract TransferLogic is BaseLogic {

    /*
    index 0: admin key
         1: asset(transfer)
         2: adding
         3: reserved(dapp)
         4: assist
     */
    uint constant internal TRANSFER_KEY_INDEX = 1;

    // Equals to ‘bytes4(keccak256("onERC721Received(address,address,uint256,bytes)"))‘
    bytes4 private constant ERC721_RECEIVED = 0x150b7a02;

    // *************** Events *************************** //

    event TransferLogicInitialised(address indexed account);
    event TransferLogicEntered(bytes data, uint256 indexed nonce);

    // *************** Constructor ********************** //
    //@CTK NO_ASF
    constructor(AccountStorage _accountStorage)
    BaseLogic(_accountStorage)
    public
  {
  }

    // *************** Initialization ******************** //

    // enable staic call ’onERC721Received’ from base account
    //@CTK NO_ASF
    function initAccount(Account _account) external allowAccountCallsOnly(_account){
        _account.enableStaticCall(address(this), ERC721_RECEIVED);
        emit TransferLogicInitialised(address(_account));
    }

    // *************** action entry ******************** //
    function enter(bytes calldata _data, bytes calldata _signature, uint256 _nonce) external {
        address account = getSignerAddress(_data);
        checkKeyStatus(account, TRANSFER_KEY_INDEX);

        address assetKey = accountStorage.getKeyData(account, TRANSFER_KEY_INDEX);
        checkAndUpdateNonce(assetKey, _nonce);
        bytes32 signHash = getSignHash(_data, _nonce);
        verifySig(assetKey, _signature, signHash);

        // solium-disable-next-line security/no-low-level-calls
        (bool success,) = address(this).call(_data);
        require(success, "calling self failed");
        emit TransferLogicEntered(_data, _nonce);
    }

    // *************** transfer assets ********************* //

    // called from 'enter'
    // signer is '_from'
    function transferEth(address payable _from, address _to, uint256 _amount) external allowSelfCallsOnly {
        Account(_from).invoke(_to, _amount, "");
    }

    // called from 'enter'
    // signer is '_from'
    function transferErc20(address payable _from, address _to, address _token, uint256 _amount) external allowSelfCallsOnly {
        bytes memory methodData = abi.encodeWithSignature("transfer(address,uint256)", _to, _amount);
        Account(_from).invoke(_token, 0, methodData);
    }

    // called from 'enter'
    // signer is '_approvedSpender'
    // make sure '_from' has approved allowance to '_approvedSpender'
    function transferApprovedErc20(address payable _approvedSpender, address _from, address _to, address _token, uint256 _amount) external allowSelfCallsOnly {
        bytes memory methodData = abi.encodeWithSignature("transferFrom(address,address,uint256)", _from, _to, _amount);
        Account(_approvedSpender).invoke(_token, 0, methodData);
    }

    // called from 'enter'
    // signer is '_from'
    function transferNft(
        address payable _from, address _to, address _nftContract, uint256 _tokenId, bytes calldata _data, bool _safe)
        external
        allowSelfCallsOnly
    {
        bytes memory methodData;
        if(_safe) {
            methodData = abi.encodeWithSignature("safeTransferFrom(address,address,uint256,bytes)", _from, _to, _tokenId, _data);
        } else {
            methodData = abi.encodeWithSignature("transferFrom(address,address,uint256)", _from, _to, _tokenId);
        }
        Account(_from).invoke(_nftContract, 0, methodData);
    }

    // called from 'enter'
    // signer is '_approvedSpender'
    // make sure '_from' has approved nftToken to '_approvedSpender'
    function transferApprovedNft(
        address payable _approvedSpender, address _from, address _to, address _nftContract, uint256 _tokenId, bytes calldata _data, bool _safe)
        external
        allowSelfCallsOnly
    {
        bytes memory methodData;
        if(_safe) {
            methodData = abi.encodeWithSignature("safeTransferFrom(address,address,uint256,bytes)", _from, _to, _tokenId, _data);
        } else {
            methodData = abi.encodeWithSignature("transferFrom(address,address,uint256)", _from, _to, _tokenId);
        }
        Account(_approvedSpender).invoke(_nftContract, 0, methodData);
    }

    // *************** callback of safeTransferFrom ********************* //
    //@CTK NO_ASF
    function onERC721Received(address _operator, address _from, uint256 _tokenId, bytes calldata _data) external pure returns (bytes4) {
        return ERC721_RECEIVED;
    }
}
```

File logics/base/AccountBaseLogic.sol

```
pragma solidity ^0.5.4;

import "./BaseLogic.sol";

contract AccountBaseLogic is BaseLogic {

    uint256 constant internal DELAY_CHANGE_ADMIN_KEY = 21 days;
    uint256 constant internal DELAY_CHANGE_OPERATION_KEY = 7 days;
    uint256 constant internal DELAY_UNFREEZE_KEY = 7 days;
    uint256 constant internal DELAY_CHANGE_BACKUP = 21 days;
    uint256 constant internal DELAY_CHANGE_ADMIN_KEY_BY_BACKUP = 30 days;

    uint256 constant internal MAX_DEFINED_BACKUP_INDEX = 5;

  // Equals to bytes4(keccak256("changeAdminKey(address,address)"))
  bytes4 internal constant CHANGE_ADMIN_KEY = 0xd595d935;
  // Equals to bytes4(keccak256("changeAdminKeyByBackup(address,address)"))
  bytes4 internal constant CHANGE_ADMIN_KEY_BY_BACKUP = 0xfdd54ba1;
  // Equals to bytes4(keccak256("changeAdminKeyWithoutDelay(address,address)"))
  bytes4 internal constant CHANGE_ADMIN_KEY_WITHOUT_DELAY = 0x441d2e50;
  // Equals to bytes4(keccak256("changeAllOperationKeys(address,address[])"))
  bytes4 internal constant CHANGE_ALL_OPERATION_KEYS = 0xd3b9d4d6;
  // Equals to bytes4(keccak256("unfreeze(address)"))
  bytes4 internal constant UNFREEZE = 0x45c8b1a6;

    event ProposalExecuted(address indexed client, address indexed proposer, bytes functionData);

    // *************** Constructor ********************** //
    //@CTK NO_ASF
  constructor(AccountStorage _accountStorage)
    BaseLogic(_accountStorage)
    public
  {
  }

    // *************** Proposal ********************** //

    /* ’executeProposal’ is shared by AccountLogic and DualsigsLogic,
       proposed actions called from ’executeProposal’:
        AccountLogic: changeAdminKeyByBackup
        DualsigsLogic: changeAdminKeyWithoutDelay, changeAllOperationKeysWithoutDelay, unfreezeWithoutDelay
    */
    function executeProposal(address payable _client, address _proposer, bytes calldata _functionData) external {
        bytes4 proposedActionId = getMethodId(_functionData);
        bytes32 functionHash = keccak256(_functionData);

        checkApproval(_client, _proposer, proposedActionId, functionHash);

        // call functions with/without delay
        // solium-disable-next-line security/no-low-level-calls
        (bool success,) = address(this).call(_functionData);
        require(success, "executeProposal failed");

        accountStorage.clearProposalData(_client, _proposer, proposedActionId);
        emit ProposalExecuted(_client, _proposer, _functionData);
    }
    function checkApproval(address _client, address _proposer, bytes4 _proposedActionId, bytes32 _functionHash) internal view {
        bytes32 hash = accountStorage.getProposalDataHash(_client, _proposer, _proposedActionId);
        require(hash == _functionHash, "proposal hash unmatch");

        uint256 backupCount;
        uint256 approvedCount;
        address[] memory approved = accountStorage.getProposalDataApproval(_client, _proposer, _proposedActionId);
        require(approved.length > 0, "no approval");

        // iterate backup list
        for (uint256 i = 0; i <= MAX_DEFINED_BACKUP_INDEX; i++) {
            address backup = accountStorage.getBackupAddress(_client, i);
            uint256 effectiveDate = accountStorage.getBackupEffectiveDate(_client, i);
            uint256 expiryDate = accountStorage.getBackupExpiryDate(_client, i);
            if (backup != address(0) && isEffectiveBackup(effectiveDate, expiryDate)) {
                // count how many backups in backup list
                backupCount += 1;
                // iterate approved array
                for (uint256 k = 0; k < approved.length; k++) {
                    if (backup == approved[k]) {
                        // count how many approved backups still exist in backup list
                        approvedCount += 1;
                    }
                }
            }
        }
        require(backupCount > 0, "no backup in list");
        uint256 threshold = SafeMath.ceil(backupCount*6, 10);
        require(approvedCount >= threshold, "must have 60% approval at least");
    }
    function checkRelation(address _client, address _backup) internal view {
        require(_backup != address(0), "backup cannot be 0x0");
        require(_client != address(0), "client cannot be 0x0");
        bool isBackup;
        for (uint256 i = 0; i <= MAX_DEFINED_BACKUP_INDEX; i++) {
            address backup = accountStorage.getBackupAddress(_client, i);
            uint256 effectiveDate = accountStorage.getBackupEffectiveDate(_client, i);
            uint256 expiryDate = accountStorage.getBackupExpiryDate(_client, i);
            // backup match and effective and not expired
            if (_backup == backup && isEffectiveBackup(effectiveDate, expiryDate)) {
                isBackup = true;
                break;
            }
        }
        require(isBackup, "backup does not exist in list");
    }
    //@CTK NO_ASF
    function isEffectiveBackup(uint256 _effectiveDate, uint256 _expiryDate) internal view returns(bool) {
        return (_effectiveDate <= now) && (_expiryDate > now);
    }
    function clearRelatedProposalAfterAdminKeyChanged(address payable _client) internal {
        //clear any existing proposal proposed by both, proposer is _client
        accountStorage.clearProposalData(_client, _client, CHANGE_ADMIN_KEY_WITHOUT_DELAY);

        //clear any existing proposal proposed by backup, proposer is one of the backups
        for (uint256 i = 0; i <= MAX_DEFINED_BACKUP_INDEX; i++) {
            address backup = accountStorage.getBackupAddress(_client, i);
            uint256 effectiveDate = accountStorage.getBackupEffectiveDate(_client, i);
            uint256 expiryDate = accountStorage.getBackupExpiryDate(_client, i);
            if (backup != address(0) && isEffectiveBackup(effectiveDate, expiryDate)) {
                accountStorage.clearProposalData(_client, backup, CHANGE_ADMIN_KEY_BY_BACKUP);
            }
        }
    }

}
```

File logics/base/BaseLogic.sol

```
pragma solidity ^0.5.4;

import "../../Account.sol";
import "../../AccountStorage.sol";
import "../../utils/SafeMath.sol";

contract BaseLogic {

    bytes constant internal SIGN_HASH_PREFIX = "\x19Ethereum Signed Message:\n32";

    mapping (address => uint256) keyNonce;
    AccountStorage public accountStorage;

    modifier allowSelfCallsOnly() {
        require (msg.sender == address(this), "only internal call is allowed");
        _;
    }

    modifier allowAccountCallsOnly(Account _account) {
        require(msg.sender == address(_account), "caller must be account");
        _;
    }

    event LogicInitialised(address wallet);

    // *************** Constructor ********************** //

    constructor(AccountStorage _accountStorage) public {
        accountStorage = _accountStorage;
    }

    // *************** Initialization ********************* //
    //@CTK NO_ASF
    function initAccount(Account _account) external allowAccountCallsOnly(_account){
        emit LogicInitialised(address(_account));
    }

    // *************** Getter ********************** //
    //@CTK NO_ASF
    function getKeyNonce(address _key) external view returns(uint256) {
        return keyNonce[_key];
    }

    // *************** Signature ********************** //
    function getSignHash(bytes memory _data, uint256 _nonce) internal view returns(
        bytes32) {
        // use EIP 191
        // 0x1900 + this logic address + data + nonce of signing key
        bytes32 msgHash = keccak256(abi.encodePacked(byte(0x19), byte(0), address(this)
            , _data, _nonce));
        bytes32 prefixedHash = keccak256(abi.encodePacked(SIGN_HASH_PREFIX, msgHash));
        return prefixedHash;
    }
    function verifySig(address _signingKey, bytes memory _signature, bytes32 _signHash
        ) internal pure {
        require(_signingKey != address(0), "invalid signing key");
        address recoveredAddr = recover(_signHash, _signature);
        require(recoveredAddr == _signingKey, "signature verification failed");
    }

    /**
     * @dev Returns the address that signed a hashed message (‘hash‘) with
     * ‘signature‘. This address can then be used for verification purposes.
     *
     * The ‘ecrecover‘ EVM opcode allows for malleable (non-unique) signatures:
     * this function rejects them by requiring the ‘s‘ value to be in the lower
     * half order, and the ‘v‘ value to be either 27 or 28.
     *
     * NOTE: This call _does not revert_ if the signature is invalid, or
     * if the signer is otherwise unable to be retrieved. In those scenarios,
     * the zero address is returned.
     *
     * IMPORTANT: ‘hash‘ _must_ be the result of a hash operation for the
     * verification to be secure: it is possible to craft signatures that
     * recover to arbitrary addresses for non-hashed data. A safe way to ensure
     * this is by receiving a hash of the original message (which may otherwise)
     * be too long), and then calling {toEthSignedMessageHash} on it.
     */
    function recover(bytes32 hash, bytes memory signature) internal pure returns (
        address) {
        // Check the signature length
        if (signature.length != 65) {
            return (address(0));
        }

        // Divide the signature in r, s and v variables
        bytes32 r;
        bytes32 s;
        uint8 v;

        // ecrecover takes the signature parameters, and the only way to get them
        // currently is to use assembly.
        // solhint-disable-next-line no-inline-assembly
        assembly {
            r := mload(add(signature, 0x20))
            s := mload(add(signature, 0x40))
            v := byte(0, mload(add(signature, 0x60)))
        }

        // EIP-2 still allows signature malleability for ecrecover(). Remove this possibility and make the signature
        // unique. Appendix F in the Ethereum Yellow paper (https://ethereum.github.io/yellowpaper/paper.pdf), defines
        // the valid range for s in (281): 0 < s < secp256k1n / 2 + 1, and for v in (282): v \in {27, 28}. Most
        // signatures from current libraries generate a unique signature with an s-value in the lower half order.
        //
        // If your library generates malleable signatures, such as s-values in the upper range, calculate a new s-value
        // with 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141 - s1 and flip v from 27 to 28 or
        // vice versa. If your library also generates signatures with 0/1 for v instead 27/28, add 27 to v to accept
        // these malleable signatures as well.
        if (uint256(s) > 0x7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF5D576E7357A4501DDFE92F46681B20A0) {
            return address(0);
        }

        if (v != 27 && v != 28) {
            return address(0);
        }

        // If the signature is valid (and not malleable), return the signer address
        return ecrecover(hash, v, r, s);
    }

    /* get signer address from data
    * @dev Gets an address encoded as the first argument in transaction data
    * @param b The byte array that should have an address as first argument
    * @returns a The address retrieved from the array
    */
    //@CTK NO_ASF
    function getSignerAddress(bytes memory _b) internal pure returns (address _a) {
        require(_b.length >= 36, "invalid bytes");
        // solium-disable-next-line security/no-inline-assembly
        assembly {
            let mask := 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
            _a := and(mask, mload(add(_b, 36)))
            // b = {length:32}{method sig:4}{address:32}{...}
            // 36 is the offset of the first parameter of the data, if encoded properly.
            // 32 bytes for the length of the bytes array, and the first 4 bytes for the function signature.
            // 32 bytes is the length of the bytes array!!!!
        }
    }

    // get method id, first 4 bytes of data
    function getMethodId(bytes memory _b) internal pure returns (bytes4 _a) {
        require(_b.length >= 4, "invalid data");
        // solium-disable-next-line security/no-inline-assembly
        assembly {
            // 32 bytes is the length of the bytes array
            _a := mload(add(_b, 32))
        }
    }

    function checkKeyStatus(address _account, uint256 _index) internal {
        // check operation key status
        if (_index > 0) {
            require(accountStorage.getKeyStatus(_account, _index) != 1, "frozen key");
        }
    }

    // _nonce is timestamp in microsecond(1/1000000 second)
    function checkAndUpdateNonce(address _key, uint256 _nonce) internal {
        require(_nonce > keyNonce[_key], "nonce too small");
        require(SafeMath.div(_nonce, 1000000) <= now + 86400, "nonce too big"); // 86400=24*3600 seconds

        keyNonce[_key] = _nonce;
    }
}
```

File testUtils/MyToken.sol

```
pragma solidity ^0.5.0;

// import "openzeppelin-solidity/contracts/token/ERC20/ERC20Detailed.sol";
import "openzeppelin-solidity/contracts/token/ERC20/ERC20Mintable.sol";

contract MyToken is ERC20Mintable {
  string private _name;
    string private _symbol;
    uint8 private _decimals;
  uint256 public val;

  constructor(string memory name, string memory symbol, uint8 decimals/*, address account, uint256 amount*/) public {
        _name = name;
        _symbol = symbol;
        _decimals = decimals;
        // mint(account, amount);
  }
```

```

    /**
     * @dev Returns the name of the token.
     */
     //@CTK NO_ASF
    function name() public view returns (string memory) {
        return _name;
    }

    /**
     * @dev Returns the symbol of the token, usually a shorter version of the
     * name.
     */
     //@CTK NO_ASF
    function symbol() public view returns (string memory) {
        return _symbol;
    }

    /**
     * @dev Returns the number of decimals used to get its user representation.
     * For example, if ‘decimals‘ equals ‘2‘, a balance of ‘505‘ tokens should
     * be displayed to a user as ‘5,05‘ (‘505 / 10 ** 2‘).
     *
     * Tokens usually opt for a value of 18, imitating the relationship between
     * Ether and Wei.
     *
     * > Note that this information is only used for _display_ purposes: it in
     * no way affects any of the arithmetic of the contract, including
     * ‘IERC20.balanceOf‘ and ‘IERC20.transfer‘.
     */
     //@CTK NO_ASF
    function decimals() public view returns (uint8) {
        return _decimals;
    }

}
```

CERTIK

Building Fully Trustworthy Smart Contracts and Blockchain Ecosystems