








SMART CONTRACT AUDIT (STND TOKEN)

Report for: Standart
Date: 27 April 2020

SEVERITY DEFINITION

The level of criticality of each risk is determined based on the potential impact of loss from successful exploitation as well as ease of exploitation, existence of exploits in public access and other factors.

The risk classification has been made on the following 5-value scale:

Critical 	Vulnerabilities that possess the highest impact over the systems, services and/or sensitive information. The existence of these vulnerabilities is dangerous and should be fixed as soon as possible
High 	Vulnerabilities that could compromise severely the service or the information it manages even if the vulnerability requires expertise to be exploited.
Medium 	Vulnerabilities that on their own could have a limited impact or that combined with other vulnerabilities could have a greater impact.
Low 	These vulnerabilities do not pose a real risk for the systems. Also includes vulnerabilities which are extremely hard to exploit or whose impact on the service is low.
Info 	It covers multiple characteristics, information or behaviours that could be considered as inappropriate, without being considered as vulnerabilities.

STRUCTURE OF CONTRACT STANDART.SOL SOW 1

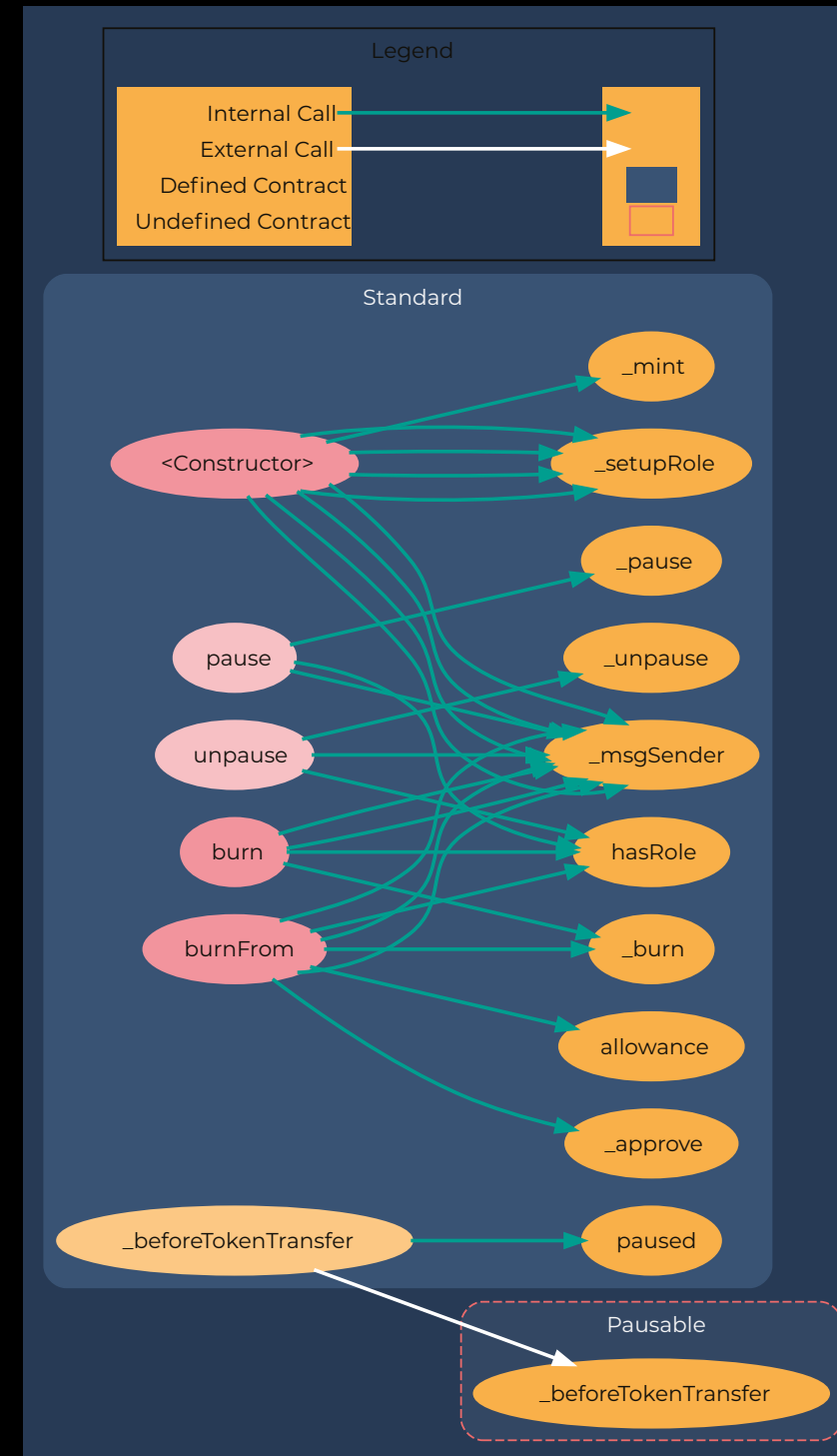


Рис. 1.1.
Standart.sol

METHODOLOGY

#	Name	Description
1	contracts/token/STND/AbstractStandartToken.sol https://github.com/digitalnativeinc/standard-evm	Revision: https://github.com/digitalnativeinc/standard-evm/blob/81f1d57cadcb0e37b49547e9ebf51aaf95bdc00a/contracts/token/STND/AbstractStandartToken.sol
2	contracts/token/STND/SNDTToken.sol https://github.com/digitalnativeinc/standard-evm	Revision: https://github.com/digitalnativeinc/standard-evm/blob/81f1d57cadcb0e37b49547e9ebf51aaf95bdc00a/contracts/token/STND/SNDTToken.sol

We've performed a series of auto tests based on SWC recommendations. Additionally there was a manual investigation of the business processes beneath of the scoped contract. Based on the results of the investigation we can ensure that the base token mechanics is correct.

STANDARD

Found 1 low problem in a file: A floating pragma is set, SWC-103

| | <Constructor> | Public | Function can modify state | ERC20 AbstractStandartToken |

Found 0 problems.

| | pause | External | Function can modify state | NO | Found 0 problems.

| | unpause | External | Function can modify state | NO | Found 0 problems.

| | _beforeTokenTransfer | Internal | Function can modify state | | Found 0 problems.

| | burn | Public | Function can modify state | NO |

Found 0 problems.

| | burnFrom | Public | Function can modify state | NO | Found 0 problems.

FROM ABSTRACTSTANDARTTOKEN

| | <Constructor> | Public | Function can modify state |NO | Found 0 problems.
| | decimals | Public | |NO |
Found 0 problems.

FROM PAUSABLE

| | <Constructor> | Public | Function can modify state | NO |

Found 0 problems.

| | paused | Public | | NO |

Found 0 problems.

| | _pause | Internal | Function can modify state | whenNotPaused |

Found 0 problems.

| | _unpause | Internal | Function can modify state | whenPaused |

Found 0 problems.

FROM

ACCESSCONTROLNUMERABLE

| | getRoleMember | Public | |NO |

Found 0 problems.

| | getRoleMemberCount | Public |

Found 0 problems.

| | grantRole | Public | Function can modify state |NO | Found 0 problems.

| | revokeRole | Public | Function can modify state |NO | Found 0 problems.

| | renounceRole | Public | Function can modify state |NO | Found 0 problems.

|NO |

| | _setupRole | Internal | Function can modify state | | Found 0 problems.

FROM ACCESSCONTROL

| | hasRole | Public | |NO |

Found 0 problems.

| | _checkRole | Internal | | |

Found 0 problems.

| | getRoleAdmin | Public | |NO |

Found 0 problems.

| | grantRole | Public | Function can modify state | onlyRole | Found 0 problems.

| | revokeRole | Public | Function can modify state | onlyRole | Found 0 problems.

| | renounceRole | Public | Function can modify state |NO | Found 0 problems.

| | _setupRole | Internal | Function can modify state | |

Found 0 problems.

| | _setRoleAdmin | Internal | Function can modify state | | Found 0 problems.

| | _grantRole | Private | Function can modify state | |

Found 0 problems.

| | _revokeRole | Private | Function can modify state | |

Found 0 problems.

FROM CONTEXT

```
| | _msgSender | Internal | | |
```

Found 0 problems.

```
| | _msgData | Internal | | |
```

Found 0 problems.

FROM ERC20

| | <Constructor> | Public | Function can modify state |NO |

Found 0 problems.

| | name | Public | |NO |

Found 0 problems.

| | symbol | Public | |NO |

Found 0 problems.

| | decimals | Public | |NO |

Found 0 problems.

| | totalSupply | Public | |NO |

Found 0 problems.

| | balanceOf | Public | |NO |

Found 0 problems.

| | transfer | Public | Function can modify state |NO |

Found 0 problems.

| | allowance | Public | |NO |

Found 0 problems.

| | approve | Public | Function can modify state |NO |

Found 0 problems.

| | transferFrom | Public | Function can modify state |NO | Found 0 problems.

| | increaseAllowance | Public | Function can modify state |NO |

Found 0 problems.

| | decreaseAllowance | Public | Function can modify state |NO | Found 0 problems.

| | _transfer | Internal | Function can modify state | |

Found 0 problems.

| | _mint | Internal | Function can modify state | |

Found 0 problems.

| | _burn | Internal | Function can modify state | |

Found 0 problems.

| | _approve | Internal | Function can modify state | |

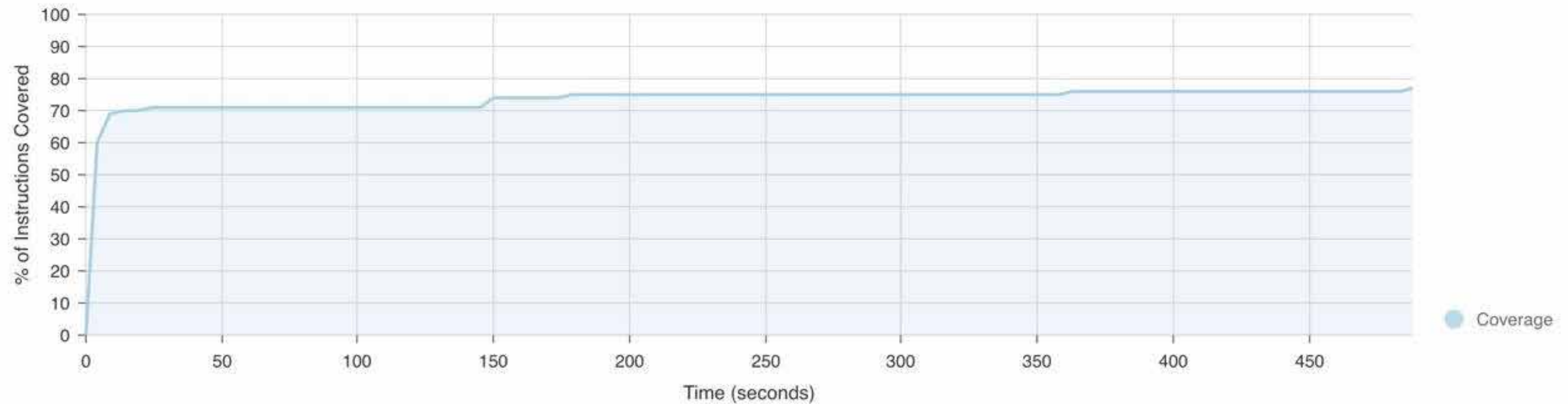
Found 0 problems.

| | _beforeTokenTransfer | Internal | Function can modify state | | Found 0 problems.

METHODOLOGY

Coverage

This graph shows the progression of coverage.



EXECUTIVE SUMMARY

Based on our understanding contract, as well as the nature of the vulnerabilities discovered, their exploitability, and the potential impact we have assessed the level of risk for your organisation to be Low

Overall security rating: High.



GET IN TOUCH

info@smartstate.tech
smartstate.tech