# DutchX Badge

This badge is used as a due diligence tool for the DutchX.
Tokens with this badge:

- Are displayed first on some of the DutchX interfaces.
- Can request the dxDAO to whitelist them for Magnolia (MGN) generation.

## Guidelines:

**Active project** The token corresponds to a real active project. This can be demonstrated by the following: *(Only one stipulation is required)*

1. The token is usable in an application and this application was used at least once during the last 30 UTC days.
   *Accept if: The token acts as a payment token in a Dapp in production with users.*
2. There is a significant amount of open source code in development and new open source code was released during the last 30 UTC days.
   *Accept if: There are 5000 lines of original and useful code on the project Github. The last commit was 5 days ago.*

**Correct price** The token is trading at the right price. *(All stipulations are required)*

1. There has been at least 1 DutchX auction of the token on the buying and selling side in each of the last 7 UTC days before the submission.
   *Accept if: There has been 3 or 4 auctions each of the past 7 days.*
2. The token is traded on at least one of the following exchanges with a cumulative volume greater than 10 000 USD in the last 30 UTC days:
   a. The following centralized exchanges: Binance, Bitfinex/Ethfinex, Bitflyer, Bitstamp, Bittrex, Coinbase Pro, Gemini, itBit, Kraken and Poloniex.
   b. The following on-chain exchanges: Uniswap, IDEX, Bancor, DeversiFi, Etherdelta/ForkDelta, OasisDex, Kyber Network, DDEX and Radar Relay.

   *Accept if: The token is traded on uniswap with a volume of 1000$ on each of the past 30 UTC days.*
3. The final price of all auctions in the last 7 UTC days before the submission is comprised between 0.5 and 2 times the market price. The market price is the average price of the token on exchanges listed in the previous criterion weighted by daily volume.
   *Accept if: The token has been trading on DutchX at prices between 0.8 and 1.1 of market price previously defined.*

**Secure contract** The contracts are unlikely to have vulnerabilities. For the purpose of this section, “contracts” refer to the token contract, contracts it relies on and contracts which have authority toward it. *(All stipulations are required)*

1. There are no vulnerabilities in the contracts which would allow to burn tokens, block transfers or create a high amount of tokens.
   *Reject if: Someone found a way to block token transfers.*
2. The contracts should have undertaken an external security audit (with public results) or a public bug bounty program published on a dedicated external platform.
   *Accept if: The contracts were audited by Consensys Diligence and do not concern a Consensys project.*
3. There isn’t a small group of actors (such as an external address or a multisig) able to create a high amount of tokens, burn tokens of other accounts or block transfers.
   *Reject if: The token contract has a “controller” which is able to create an arbitrary amount of tokens. This “controller” is a multisig.*