CERTIK

Confidential

Kortana

KYC Diligence Report

Delivered on: May 18, 2023

Project Team: Kortana

Executive Summary

This report provides a comprehensive overview of the records and findings from the KYC due diligence for **Kortana**. It includes 4 individual data records, a KYC submissions analysis, a preliminary risk assessment of the team, an intelligence risk assessment of the team, an on-chain investigation and analysis, a geographical risk assessment, a security interview report, an open-source investigation report, and an adjudication report. All of these records and risk assessments are examined independently and considered jointly to make a final risk evaluation for the project based on all pertinent elements and risk metrics.

Kortana passed the following checks:

- ✓ Team Identity Verification
- ✓ Individual Records Analysis
- ✓ AML/Watchlist Screenings
- ✓ Sanctions Review
- ✓ Criminal History Check
- ✓ Country Risk Assessment
- ✓ Preliminary Team Risk Assessment
- ✓ Intelligence Team Risk Assessment
- ✓ On-Chain Wallet Review
- ✓ Open Source Research (OSINT)
- ✓ Founder Security Interview

Based on the comprehensive risk assessment, Kortana qualifies for a **Silver KYC badge**.
This result can be verified on the CertiK website:

https://skynet.certik.com/

https://skynet.certik.com/leaderboards/kyc

Report Format

CertiK has organized the report into seven sections, each providing a different security outlook: Personal Data Records and Analysis, KYC Submissions Analysis, Preliminary Team Risk Assessment, Intelligence Team Risk Assessment, Security Interview Findings, Open-Source Investigation Findings, Adjudication Report, and Anti-Money Laundering and Terrorist Financing Controls. Additional information is provided in the Appendix at the end of this report.

Table of Contents

Personal Data Records & Analysis

Verified Team Member #01

Data	Records
Declared Project name	Confidential Information
Declared Last name	Confidential Information
Matching last name with ID	Confidential Information
Declared First name	Confidential Information
Matching first name with ID	Confidential Information
Declared date of birth	Confidential Information
Matching of date of birth on ID	Confidential Information
Declared place of birth	Confidential Information
Matching place of birth on ID	Confidential Information
Declared residential address	Confidential Information
Matching residential address with IP address	Confidential Information
Declared country	Confidential Information
Matching country with IP address	Confidential Information
ID document type	Confidential Information
ID document/Image quality	Confidential Information
Fraudulent submission patterns	Confidential Information
Document date	Confidential Information
ID document number	Confidential Information
ID validity date	Confidential Information
Document blocklisted	Confidential Information
Successful data comparison	Confidential Information
Facial check detection	Confidential Information
Comparison face/ID	Confidential Information
AI Liveness check	Confidential Information
Namecheck for warning lists	Confidential Information
Namecheck for sanctions lists	Confidential Information
Namecheck for watchlists	Confidential Information
Namecheck for politically exposed persons	Confidential Information
Namecheck for Persons and Entities of Special Interest	Confidential Information
Namecheck for adverse media	Confidential Information
Verification of the email address	Confidential Information
Declared Twitter username	Confidential Information
Declared Telegram username	Confidential Information
Declared project wallet address(es)	Confidential Information
Declared project inception date	Confidential Information
Declared holder of private key(s)	Confidential Information
Test transaction hash	Confidential Information
Proof of domain ownership	Confidential Information
CV/Resume/Professional bio	Confidential Information
Data collection agreement	Confidential Information

Verified Team Member #01 (2/2)

Data	Records
Submission timestamp	Confidential Information
IP address(es) for the submission	Confidential Information
Country of connection	Confidential Information
City of connection	Confidential Information
Telephone number	Confidential Information
Verification of the telephone number	Confidential Information
Metadata of uploaded documents	Confidential Information

Verified Team Member #02

Data	Records
Declared Project name	Confidential Information
Declared Last name	Confidential Information
Matching last name with ID	Confidential Information
Declared First name	Confidential Information
Matching first name with ID	Confidential Information
Declared date of birth	Confidential Information
Matching of date of birth on ID	Confidential Information
Declared place of birth	Confidential Information
Matching place of birth on ID	Confidential Information
Declared residential address	Confidential Information
Matching residential address with IP address	Confidential Information
Declared country	Confidential Information
Matching country with IP address	Confidential Information
ID document type	Confidential Information
ID document/Image quality	Confidential Information
Fraudulent submission patterns	Confidential Information
Document date	Confidential Information
ID document number	Confidential Information
ID validity date	Confidential Information
Document blocklisted	Confidential Information
Successful data comparison	Confidential Information
Facial check detection	Confidential Information
Comparison face/ID	Confidential Information
AI Liveness check	Confidential Information
Namecheck for warning lists	Confidential Information
Namecheck for sanctions lists	Confidential Information
Namecheck for watchlists	Confidential Information
Namecheck for politically exposed persons	Confidential Information
Namecheck for Persons and Entities of Special Interest	Confidential Information
Namecheck for adverse media	Confidential Information
Verification of the email address	Confidential Information
Declared Twitter username	Confidential Information
Declared Telegram username	Confidential Information
CV/Resume/Professional bio	Confidential Information
Data collection agreement	Confidential Information

Verified Team Member #03

Data	Records
Declared Project name	Confidential Information
Declared Last name	Confidential Information
Matching last name with ID	Confidential Information
Declared First name	Confidential Information
Matching first name with ID	Confidential Information
Declared date of birth	Confidential Information
Matching of date of birth on ID	Confidential Information
Declared place of birth	Confidential Information
Matching place of birth on ID	Confidential Information
Declared residential address	Confidential Information
Matching residential address with IP address	Confidential Information
Declared country	Confidential Information
Matching country with IP address	Confidential Information
ID document type	Confidential Information
ID document/Image quality	Confidential Information
Fraudulent submission patterns	Confidential Information
Document date	Confidential Information
ID document number	Confidential Information
ID validity date	Confidential Information
Document blocklisted	Confidential Information
Successful data comparison	Confidential Information
Facial check detection	Confidential Information
Comparison face/ID	Confidential Information
AI Liveness check	Confidential Information
Namecheck for warning lists	Confidential Information
Namecheck for sanctions lists	Confidential Information
Namecheck for watchlists	Confidential Information
Namecheck for politically exposed persons	Confidential Information
Namecheck for Persons and Entities of Special Interest	Confidential Information
Namecheck for adverse media	Confidential Information
Verification of the email address	Confidential Information
Declared Twitter username	Confidential Information
Declared Telegram username	Confidential Information
CV/Resume/Professional bio	Confidential Information
Data collection agreement	Confidential Information

Verified Team Member #04

Data	Records
Declared Project name	Confidential Information
Declared Last name	Confidential Information
Matching last name with ID	Confidential Information
Declared First name	Confidential Information
Matching first name with ID	Confidential Information
Declared date of birth	Confidential Information
Matching of date of birth on ID	Confidential Information
Declared place of birth	Confidential Information
Matching place of birth on ID	Confidential Information
Declared residential address	Confidential Information
Matching residential address with IP address	Confidential Information
Declared country	Confidential Information
Matching country with IP address	Confidential Information
ID document type	Confidential Information
ID document/Image quality	Confidential Information
Fraudulent submission patterns	Confidential Information
Document date	Confidential Information
ID document number	Confidential Information
ID validity date	Confidential Information
Document blocklisted	Confidential Information
Successful data comparison	Confidential Information
Facial check detection	Confidential Information
Comparison face/ID	Confidential Information
AI Liveness check	Confidential Information
Namecheck for warning lists	Confidential Information
Namecheck for sanctions lists	Confidential Information
Namecheck for watchlists	Confidential Information
Namecheck for politically exposed persons	Confidential Information
Namecheck for Persons and Entities of Special Interest	Confidential Information
Namecheck for adverse media	Confidential Information
Verification of the email address	Confidential Information
Declared Twitter username	Confidential Information
Declared Telegram username	Confidential Information
CV/Resume/Professional bio	Confidential Information
Data collection agreement	Confidential Information

KYC Submissions Analysis

KYC Submissions Summary

CertiK requires that all key team members submit personal KYC information, including the Smart Contract Developer or CTO, to maximize accountability and transparency. All team members that KYC'd for Kortana passed 33 evaluation standards, including watchlist checks and digital authenticity verification. In total, Kortana provided 4 KYC submissions.

Identity Verification

The 4 KYC submissions that Kortana submitted passed the identity verification. No watchlist or AML/CTF concerns were noted.

Country Risk

The country risk for Kortana evaluated to be **Tier 2** based. Country Risk refers to a project team's geographical risk and the risk associated with the location and distribution of a project team. The location of the project team and its members is confidential and is not publicly disclosed on the KYC Badge or the CertiK website. Geographical risk is determined based on an aggregation of official international risk ratings and projects are assigned Tier 1, Tier 2, or Tier 3 according to the following framework:

Geographical Analysis for the Core Team	
Tier 1	The core team is situated in country(ies) that received the most secure, aggregated ratings based on its international judicial cooperation, criminal justice system, anti-money laundering statutes, and corruption. This contextual data suggests the highest level of geographic accountability, thus maximizing risk reduction and mitigation.
Tier 2	The core team is situated in country(ies) that received medium aggregated ratings based on its international judicial cooperation, criminal justice system, anti-money laundering statutes, and corruption. This contextual data suggests a medium level of geographic accountability, thus reducing and mitigating the risk of fraud.
Tier 3	The core team is situated in country(ies) that received low aggregated ratings based on its international judicial cooperation, criminal justice system, anti-money laundering statutes, and corruption. This contextual data suggests an increased difficulty and complexity in preventing and mitigating fraud.

Preliminary Team Risk Assessment

PTRA Risk Assessment

Preliminary Risk Metrics	Weighted Risk Scores
1. Behavioral risk assessment (10% of the PTRA)	
✓ Risk factor PTRA/RF11	Confidential Information
✓ Risk factor PTRA/RF12	Confidential Information
✓ Risk factor PTRA/RF13	Confidential Information
2. Core team identification risk (27% of the PTRA)	
✓ Risk factor PTRA/RF21	Confidential Information
✓ Risk factor PTRA/RF22.	Confidential Information
✓ Risk factor PTRA/RF23	Confidential Information
✓ Risk factor PTRA/RF24	Confidential Information
✓ Risk factor PTRA/RF25	Confidential Information
✓ Risk factor PTRA/RF26	Confidential Information
✓ Risk factor PTRA/RF27	Confidential Information
✓ Risk factor PTRA/RF28	Confidential Information
3. Key tech team composition risk (10% of the PTRA)	
✓ Risk factor PTRA/RF31	Confidential Information
✓ Risk factor PTRA/RF32	Confidential Information
✓ Risk factor PTRA/RF33	Confidential Information
4. Background history concealment risk (13% of the PTRA)	
✓ Risk factor PTRA/RF41	Confidential Information
✓ Risk factor PTRA/RF42	Confidential Information
✓ Risk factor PTRA/RF43	Confidential Information
✓ Risk factor PTRA/RF44	Confidential Information
5. Background activity risk assessment (10% of the PTRA)	
✓ Risk factor PTRA/RF51	Confidential Information
✓ Risk factor PTRA/RF52	Confidential Information
✓ Risk factor PTRA/RF53	Confidential Information
6. Assessment of strategic team discrepancies (17% of the PTRA)	
✓ Risk factor PTRA/RF61	Confidential Information
✓ Risk factor PTRA/RF62	Confidential Information
✓ Risk factor PTRA/RF63	Confidential Information
✓ Risk factor PTRA/RF64	Confidential Information
✓ Risk factor PTRA/RF65	Confidential Information
7. Assessment of other risks/discrepancies /derogatory info (10% of the PTRA)	
✓ Risk factor PTRA/RF71	Confidential Information
✓ Risk factor PTRA/RF72	Confidential Information
✓ Risk factor PTRA/RF73	Confidential Information
Weighted Preliminary Team Risk Score (PTRA*):	Confidential Information
PTRA Risk level	**Medium**

* The PTRA risk model is detailed on the next page

Detailed Risk Model for the Preliminary Team Risk Assessment (PTRA)

Scope: The scope of this preliminary team risk assessment is not to the risk of the project itself. It measures only the risk associated with the identification and background of the core team members. This Analytical-based score evaluates the probability that the information about the team is accurate and comprehensive, and the probability that the team is concealing background elements that could have serious operational, reputational or legal consequences.

Score: 0/100 equals no risk detected during the preliminary team risk assessment - 100/100 equals maximum risk detected during the preliminary team risk assessment of the team.

Relative weighting of risk signals and categories: Every detected risk signal is weighted at detection in order to account for the weight of the signal, the mitigating factors, and aggravating factors. Every category of risk is subsequently weighted, based on the relative weight of each risk category.

Distribution of the Risk Metrics:

Categories of preliminary risk metrics	Relative weight in the PTRA	Number of risk metrics
Behavioral risk assessment	10%	3
Core team identification risk	27%	8
Key tech team composition risk	10%	3
Background history concealment risk	13%	4
Background activity risk assessment	10%	3
Assessment of strategic team discrepancies	17%	5
Assessment of other risks/discrepancies /derogatory info	10%	3
PTRA score	**100%**	**29**

Intelligence Team Risk Assessment

ITRA Risk Assessment

Intelligence Risk Metrics	Weighted Risk Scores
1. Analysis of KYC submissions (19% of the ITRA)	
✓ Risk factor ITRA/RF11	Confidential Information
✓ Risk factor ITRA/RF12	Confidential Information
✓ Risk factor ITRA/RF13	Confidential Information
✓ Risk factor ITRA/RF14	Confidential Information
✓ Risk factor ITRA/RF15	Confidential Information
✓ Risk factor ITRA/RF16	Confidential Information
✓ Risk factor ITRA/RF17	Confidential Information
2. Background history intelligence analysis (7% of the ITRA)	
✓ Risk factor ITRA/RF21	Confidential Information
✓ Risk factor ITRA/RF22	Confidential Information
✓ Risk factor ITRA/RF23	Confidential Information
3. Verifiability of the team's activities (15% of the ITRA)	
✓ Risk factor ITRA/RF31	Confidential Information
✓ Risk factor ITRA/RF32	Confidential Information
✓ Risk factor ITRA/RF33	Confidential Information
✓ Risk factor ITRA/RF34	Confidential Information
✓ Risk factor ITRA/RF35	Confidential Information
✓ Risk factor ITRA/RF36	Confidential Information
4. Social Media intelligence analysis (12% of the ITRA)	
✓ Risk factor ITRA/RF41	Confidential Information
✓ Risk factor ITRA/RF42	Confidential Information
✓ Risk factor ITRA/RF43	Confidential Information
✓ Risk factor ITRA/RF44	Confidential Information
✓ Risk factor ITRA/RF45	Confidential Information
5. On-chain behavioral risk analysis (10% of the ITRA)	
✓ Risk factor ITRA/RF51	Confidential Information
✓ Risk factor ITRA/RF52	Confidential Information
✓ Risk factor ITRA/RF53	Confidential Information
✓ Risk factor ITRA/RF54	Confidential Information
6. Strategic discrepancy analysis (7% of the ITRA)	
✓ Risk factor ITRA/RF61	Confidential Information
✓ Risk factor ITRA/RF62	Confidential Information
✓ Risk factor ITRA/RF63	Confidential Information
7. Major derogatory intelligence analysis (20% of the ITRA)	
✓ Risk factor ITRA/RF71	Confidential Information
✓ Risk factor ITRA/RF72	Confidential Information
✓ Risk factor ITRA/RF73	Confidential Information
✓ Risk factor ITRA/RF74	Confidential Information
8. Assessment of other risks/discrep./derog. info (5% of the ITRA)	
✓ Risk factor ITRA/RF81	Confidential Information
✓ Risk factor ITRA/RF82	Confidential Information
Weighted Intelligence Team Risk Assessment score (ITRA*):	Confidential Information
ITRA Risk level * The ITRA risk model is detailed on the next page	**Medium**

Detailed Risk Model for the Intelligence Team Risk Assessment (ITRA)

Scope: The scope of this intelligence team risk assessment is not to the risk of the project itself. It measures only the risk associated with the identification and background of the core team members. The intelligence-based score evaluates the probability that the information about the team is accurate and comprehensive, and the probability that the team is concealing background elements that could have serious operational, reputational or legal consequences.

Score: 0/100 equals no risk detected during the intelligence team risk assessment - 100/100 equals maximum risk detected during the intelligence team risk assessment of the team.

Relative weighting of risk signals and categories: Every detected risk signal is weighted at detection in order to account for the weight of the signal, the mitigating factors, and aggravating factors. Every category of risk is subsequently weighted, based on the relative weight of each risk category.

Distribution of the Risk Metrics:

Categories of intelligence risk metrics	Relative weight in the ITRA	Number of risk metrics
Analysis of KYC submissions	19%	7
Background history intelligence analysis	7%	3
Verifiability of the team's activities	15%	6
Social Media intelligence analysis	12%	5
On-chain behavioral risk analysis	10%	4
Strategic discrepancy analysis	7%	3
Major derogatory intelligence analysis	20%	4
Assessment of other risks/discrepancies /derogatory info	5%	2
ITRA score	100%	29

Security Interview Findings

Security Interview Summary

A professional investigator from the CertiK KYC team conducted a security interview with the person claiming to be in charge of Kortana on May 17, 2023. The CertiK security interview is a thorough process that allows the project lead to provide information on the project, the team involved, and details related to the KYC due diligence. Project owners that participate in the call do so at their own will and provide only information they are comfortable with sharing.

The security interview provides a higher level of knowledge and verification in order to detect potential issues and gather comparable intelligence about the project and the team. The security interview recording and personal information provided by the interviewee are kept confidential and are not publicly disclosed on the KYC Badge or the CertiK website.

Security Interview Key Findings

Key intelligence records and findings from the security interview for Kortana are confidentially stored by CertiK.

Open Source Investigation (OSINT) Findings

OSINT Summary

CertiK conducted a comprehensive open-source investigation of Kortana including verification of the team, on-chain analysis, and criminal history checks. The OSINT stage is conducted to also verify information detailed from the security interview. The OSINT risk assessment for Kortana found a **Medium level** of risks.

OSINT Key Findings

It was assessed that Kortana had a **Medium risk level** based on the Intelligence Team Risk Assessment Score. Key intelligence records and findings from this investigation are confidentially stored by CertiK.

Adjudication Report

Adjudication Summary

The final component of the CertiK KYC is an adjudication analysis which compiles all findings and analysis from the Personal Data Records and Analysis, KYC Submissions Analysis, Preliminary Team Risk Assessment, Intelligence Team Risk Assessment, Security Interview Findings, and Open-Source Investigation Findings. From these findings, the adjudication process results in a final risk assessment, to which the project either passes or fails the KYC. If the project passes the KYC, the project will receive one of three tier KYC badge levels: bronze, silver, or gold.

KYC Badge Award for Kortana

Based on a multi-step adjudication risk assessment, and on the criteria detailed above for each badge award, Kortana initially receives a **Silver KYC Badge**, valid for one year. This badge and associated award(s) can be removed at any time by CertiK if any fraudulent or derogatory behavior is suspected.

Upon eligibility verification, Kortana will be able to apply for a 90-day KYC Badge Award review where an additional risk assessment and evaluation on the project status and progress will be conducted. Based on the results of this review, the project may qualify for a higher badge tier. Kortana will be able to apply for this review after 90 days.

Key Adjudication Findings

Key adjudication records and findings from this investigation are confidentially stored by CertiK.

Adjudication Report (2/2)

Risk Assessment Summary

The preliminary team risk assessment and intelligence team risk assessment were considered in the final adjudication result of the KYC badge. For Kortana, the risk levels are detailed below.

Assessment Report	Risk Levels
Preliminary Team Risk Assessment	Medium
Intelligence Team Risk Assessment	Medium

The risk assessment scoring, detailed earlier in this report, measures risk associated with the identification and background of the core team members. This intelligence-based score evaluates the probability that the information about the team is accurate. The findings from the risk assessments and intelligence stages are then evaluated within the parameters of each KYC badge tier. These parameters are highlighted further below.

KYC Badge Awards Details

The CertiK KYC is a multi-step comprehensive due diligence process that determines the allocation of a KYC Badge. Only projects that successfully pass this verification process will receive a KYC Badge which can be one of three different badge awards; KYC Gold Verified, KYC Silver Verified, and KYC Bronze Verified. These badges are determined according to the below framework:

KYC Badges	
Bronze	The project team successfully passed a thorough identification and verification of selected team members, demonstrating transparency and accountability, thus reducing and mitigating the risk of fraud.
Silver	The entire core team provided identification, as well as additional, verifiable background information, indicating a higher level of transparency and accountability, and increasingly reducing and mitigating the risk of fraud.
Gold	The entire core team provided the highest amount of verifiable background information and guarantees, demonstrating a very high level of transparency and accountability, thus maximizing the risk reduction and mitigation.

Anti-Money Laundering & Terrorist-Financing Controls (1/2)

As money laundering and terrorist financing are critical risks that can adversely affect Web3 project operations, reputation, and legal compliance, it is an important aspect of the due diligence process. The CertiK KYC badge process actively scrutinizes project teams for the purpose of anti-money laundering (AML) and terrorist financing (CFT) prevention, with the following controls.

1. Verification-Based Controls

a. In depth due diligence investigation in order to determine and verify who is the core project team, its ownership of the project, and its detailed background history. Including: truly understanding the nature and purpose of the customer's business, the source of the customer's funds, and the customer's true identity or ownership.

b. Use of career professional, trained investigators and analysts in order to review and evaluate risk of fraudulent and criminal activities.

c. Maintenance of a robust, updated process and case management system for KYC investigations and risk assessments.

d. Use of a risk-based analytical process, tailored to the risk level of each customer. Use of a risk-score based system to determine the proper amount of oversight for each project (The degree of due diligence and activity monitoring is constantly proportional to the risk level).

2. Screening-Based Controls

a. Screening of the known project's wallets against the risk of association with listed fraudulent wallets and protocols. Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities.

b. Screening of the core project team with the OFAC Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists, Foreign Sanctions Evaders (FSE) List, Sectoral Sanctions Identifications (SSI) List, Palestinian Legislative Council (NS-PLC) list.

c. Screening of the core project team with the OFAC List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List), Non-SDN Menu-Based Sanctions List (NS-MBS List),

Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List), Foreign Financial Institutions Subject to Part 561 (the Part 561 List), and Non-SDN Iranian Sanctions Act (NS-ISA) List.

3. Quality Assurance and Reporting Obligations

a. Quality assurance process in place to scrutinize the investigation and verification procedures, the risk rating process, the AML/CTF and sanction checks, the KYC record keeping, and the procedures to report criminal suspicions to the authorities.

b. KYC records keeping according to FATF recommendations.

c. Reporting of AML/CFT violations as well as suspicions of money laundering and terrorist financing activities.

d. Active, direct cooperation with law enforcement in all cases of suspected criminal activity.

Disclaimer

Not Investment Advice

The information provided in this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. CertiK does not recommend that any cryptocurrency should be bought, sold, or held by you. Conduct your own due diligence and consult your financial advisor before making any investment decisions.

Privacy Policy

All information is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (integrity and confidentiality). All confidential information is treated in accordance with CertiK's applicable privacy and data protection policies.

Accuracy of Information

CertiK will strive to ensure accuracy of information listed on this report although it will not hold any responsibility for any missing or wrong information. CertiK provides all information “AS IS”. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion.

Non Endorsement

All content provided herein our report, hyperlinked sites, associated applications, forums, blogs, social media accounts and other platforms on CertiK’s report does not constitute an endorsement, guarantee, warranty, or recommendation by CertiK. Do conduct your own due diligence before deciding to use any third party services. No content on our Site is meant to be a solicitation or offer.

Official Domains

The domains certik.com, certik.io, and certik.org are official websites owned and operated by CertiK. Please verify that you are interacting with one of the following domains when visiting the Security Leaderboard or in communication with CertiK personnel.

Report Vulnerabilities

Please do not discuss any vulnerabilities, including resolved ones, outside of the program without written consent from the CertiK team. The Bug Bounty Program is assessed based on severity in accordance with the Common Vulnerability Scoring Standard (CVSS). Reach out to info@certik.com to report an issue or for general inquiries.

Process for the KYC Badge

The process for the KYC Badge is detailed here:
https://www.certik.com/resources/blog/7pSqAsYSLro9gMFeuIjPsj-how-we-do-kyc

Online authentication of KYC Badges:

Every KYC Badge can be authenticated by verifying directly on the CertiK security leaderboard here: https://www.certik.com/

KYC Badge Process

A CertiK KYC badge (a “Badge”) is issued to a project upon completion of our “know your customers (KYC)” vetting process for the project. Our vetting process is designed with the aim of de-anonymizing developers and enhancing transparency in the crypto industry. Specifically, our KYC vetting process consists of the following procedures:

1. Identity Verification. We will collect multiple forms of identification documents from members of the project and run these documents through a third-party verification platform, in order to verify ID legitimacy, conduct liveness check and obtain an individualized risk score.
2. KYC Questionnaire. We will send the project a questionnaire that collects information from persons internal to and responsible for the project as well as documentary evidence showing their roles with respect to the project.
3. Investigation & Review. We will analyze and review the information collected through the procedures set forth above.
4. Recorded Video Call. We will conduct a live, recorded meeting to live-verify all of the identification documents provided.

Validity of the KYC badge

The date indicated on this report is the date on which we have completed our KYC verification process set forth above for that project. As a result, you may not infer from the Badge that we have performed any procedures or we have renewed the KYC vetting process, in each case, at any time subsequent to the date for the Badge.

Use of the KYC Badge

Our Badge is NOT a guarantee that the information that a developer provides us is truthful or complete, that such persons will not take any malicious actions, or that we can necessarily detect frauds perpetrated with "deep fake" or other sophisticated technologies. Instead, the Badge should be viewed as what it is: it is merely an indication that we have used commercially reasonable efforts to complete our KYC procedures set forth above on the date of the Badge.

THE BADGE IS NOT A GUARANTEE FOR SAFETY. YOUR RELIANCE ON A BADGE IS SOLELY AT YOUR OWN RISK. WE ARE NOT RESPONSIBLE FOR YOUR INVESTMENT LOSS AND HEREBY EXPRESSLY DISCLAIM ANY LIABILITIES THAT MAY ARISE FROM YOUR USE OR REFERENCE OF THE BADGE.

Report a security incident

If you need immediate assistance for a possible security incident or breach, you can contact CertiK’s investigation team here: https://www.certik.com/products/incident-response

CertiK | **Securing** the **Web3** World

Learn more at www.certik.com