CERTIK

Digital Asset Registry Off-Chain Audit

Security Assessment

CertiK Assessed on Aug 21st, 2026

CertiK Assessed on Aug 21st, 2026

Digital Asset Registry Off-Chain Audit

The security assessment was prepared by CertiK.

Executive Summary

TYPES	PLATFORM	METHODS
SDK	Web Application	Dynamic Testing, Manual Review, Testnet Deployment

LANGUAGE	TIMELINE
Java, Scala	Preliminary comments published on 07/18/2026 Final report published on 08/21/2026

Vulnerability Summary

12	1	0	11	0
Total Findings	Resolved	Partially Resolved	Acknowledged	Declined

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed immediately. Users should be cautious when interacting with any application with outstanding critical risks.
0	High		High risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds, thief of user data, and/or loss control of the application.
4	Medium	4 Acknowledged	Medium risks may not pose a security risk at a large scale, but they can affect the overall functioning of a platform or be used to target a certain group of users.
6	Low	1 Resolved, 5 Acknowledged	Low risks can be any of the above, but on a smaller impact. They generally do not compromise the overall integrity of the project.
2	Informational	2 Acknowledged	Informational errors are often recommendations to improve the configuration or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the application.

SCOPE | DIGITAL ASSET REGISTRY OFF-CHAIN AUDIT

Source Code	https://github.com/DACH-NY/canton-network-utilities/tree/v0.12.15/app/backend
Source Code	https://github.com/DACH-NY/canton-network-utilities/tree/v0.12.15/app/frontend
Commit	8308beb6847d9abff36df69fbb266150d5c7e877

ENGAGEMENT SUMMARY

DIGITAL ASSET REGISTRY OFF-CHAIN AUDIT

Introduction

CertiK conducted a comprehensive security assessment of the Canton Network Off-Chain Utilities. The assessment covered the in-scope frontend and backend components under `app/frontend` and `app/backend`, with particular focus on the utility APIs, active registry and credential workflows, in-scope operator automation services, contract archival, reward processing, and other supporting off-chain functionality that interacts with the Canton ledger.

The engagement was conducted in July 2026 by three members of the CertiK team and resulted in 12 security-relevant findings across the assessed scope. The review focused on the security boundaries between externally or internally accessible off-chain services.

Methodology

During the assessment, CertiK applied industry-standard and practical security testing methodologies, including OWASP-aligned application security testing, NIST-style testing practices, and threat-model-driven analysis. The evaluation combined extensive manual source code review with dynamic testing and local deployment of the relevant services.

Testing focused on application functionality, workflow and business logic, authentication and authorization, party and operator scoping, input validation, backend resource handling, automation behavior, and security configuration. The assessment also included targeted OpenAPI-based fuzzing of the utility APIs, adversarial-input testing, and concurrency testing to evaluate the resilience of unauthenticated endpoints and determine whether malformed or repeated requests could reach backend processing or consume shared resources.

Particular attention was given to the interaction between off-chain services and Daml authorization. The review assessed whether operator-visible ledger data could be unintentionally exposed through HTTP services, whether privileged automation functionality was appropriately restricted, and whether off-chain processing correctly preserved the trust assumptions and authorization requirements of the corresponding on-ledger workflows.

Security Hardening

The assessment identified a total of 12 findings. For the utility APIs, findings mainly related to authentication and authorization gaps, information disclosure, backend resource handling, and API implementation hardening. For the in-scope automation and operational backend services, findings mainly related to access control, workflow and business logic, state consistency, security configuration, and dependency maintenance. Overall, the findings were Medium to Informational in severity, with no Critical or High severity issues observed.

The Digital Asset team collaborated effectively with CertiK during the assessment and remediation process. The project team used dedicated communication channels to iterate on findings, provide technical clarification, and review proposed mitigations.

The Canton Network Off-Chain Utilities implement an important underlying security boundary through Daml's on-ledger authorization model. Although the assessment identified several cases where off-chain services could expose operator-visible information or provide insufficiently restricted management functionality, testing did not demonstrate a bypass of the

underlying ledger authorization controls. In particular, unauthorized disclosure of credential-related information did not enable callers to act as another party or forge credentials, and no practical exploit chain leading from the identified off-chain weaknesses to unauthorized ledger actions was identified during the assessment. Dynamic testing, fuzzing, and adversarial-input testing further helped validate the behavior of the utility APIs and identify areas where additional defense-in-depth controls should be applied.

Conclusion

In conclusion, CertiK's assessment improved the overall security posture of the Canton Network Off-Chain Utilities. The assessment identified opportunities for improvement particularly around service-layer authentication and authorization, protection of privileged operational endpoints, control of information exposed through utility APIs, backend resource protections, workflow and state-consistency handling, and dependency and patch management. These improvements will help strengthen the security and resilience of the off-chain services and reduce unnecessary exposure of privileged functionality and data.

As with any complex infrastructure platform, maintaining a continuous security program through regular testing, monitoring, deployment review, dependency management, and adaptation to emerging threats will be important to support the long-term security and reliability of the Canton Network Off-Chain Utilities.

DISCLAIMER | CERTIK

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 Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with 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, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Elevate Your Web3 Journey

CertiK is the largest Web3 security platform combining formal verification with audits and comprehensive security solutions.