Kyle Den Hartog

Email: resume@kyledenhartog.com Cell Phone: +64 (027) 297-1753
Website: https://kyledenhartog.com GitHub: https://github.com/kdenhartog

Professional Experience:

Senior Software Standards Engineer **July 2019 - Present**

MATTR, Auckland, New Zealand

- Acted as a subject matter expert and a key contributor to the architecture of MATTR products. I tracked and informed the latest updates in the decentralized identity ecosystem and the relevant standards working groups such as W3C DID WG, W3C VCWG, W3C CCG DID resolution draft standard, Sidetree protocol standard, CHAPI draft standard, Open ID connect standard, and many other relevant works in the space
- Represented MATTR as a software engineer and standards working group representative in the Decentralized Identifiers Working Group and Verifiable Claims Working Group at W3C
- Authored and assisted in architecting the relevant core software libraries MATTR uses to build it's products with decentralized identifiers, verifiable credentials, DID resolution, DID registration, JSON Web Messages, and DID Communications (DIDCommV2)
- Mentored and assisted in training exercises to teach our engineering team about the relevant technologies used in the decentralized identity ecosystem. This includes topics about JSON-LD, JOSE standards, cryptography, and the standards development process
- Collaborated in the development of business strategy goals around how open standards plays into the development of our business models, products, and services
- Promoted good security practices within the organization acting as a subject matter expert for cryptography and key management. This included designing and architecting our internal key management service to securely handle cryptographic keys
- Additionally authored our internal cryptography policy and reviewed additional information security framework policies based on NZISM v3.4 in order to meet SOC2 compliance requirements
- Built proof of concepts to experiment with new functionality and keep MATTR on the cutting edge of technological updates in the space. This included the development of offline verifiable credential exchange via QR codes and NFC
- Reviewed, collaborated and maintained JSON-LD BBS+ Signatures typescript library which enabled selective disclosure via a zero knowledge proof signature scheme
- Worked directly with C suite management to keep development of MVP products on schedule for their deployment regularly assessing feature scope and making priority recommendations of what can be kept or deferred
- Discovered and responsibly disclosed a cryptographic twist attack in the secp256k1 implementation of elliptic.js which was reported under CVE-2020-28498

Blockchain Research Engineer

Evernym, Draper, UT **December 2017 - February 2019**

- Collaborated with community software architects and developers to formalize multiple community technical standards one of which was a standard message encryption format derived from JSON Web Encryption
- Contributed to the development of decentralized identifier (DIDs) authentication and authorization protocols using digital signature cryptography and zero knowledge proofs throughout the decentralized identity community
- Researched several blockchain based identity projects to determine viability of interoperability with Sovrin which led to a public partnership between Ontology and Evernym
- Mentored an intern for 6 months helping him architect and develop the first Hyperledger Indy python reference agent which
- Created and maintained the Indy-Dev repository which improved the onboarding experience for developers to test the Hyperledger Indy-SDK from hours to minutes through the use of a common docker development environment
- Researched academic papers to identify cryptographic protocols that would help with the design of a p2p encryption protocol which led to the development of the DIDCommV1 protocol and Hyperledger Aries
- Represented Evernym as a contributor to the formation of the Hyperledger Aries project

Kyle Den Hartog

Email: resume@kyledenhartog.com
Cell Phone: +64 (027) 297-1753
Website: https://kyledenhartog.com
GitHub: https://github.com/kdenhartog

Information Security Engineer I
ProCircular Inc., Iowa City, IA **May 2016 - May 2017**

- Wrote scripts, automated workflows, and improved business process efficiency to decrease vulnerability assessment times by 57.4%
- Efficiently conducted vulnerability assessments, external penetration tests, web application testing assessments, and red team engagements to help the company reach profitability within 6 months
- Executed from concept to delivery a program for executive training on cybersecurity awareness in 3 months
- Delivered on time custom client reports with documented analysis of findings, vulnerabilities, exploits, gaps, risks, and recommendations that could be easily interpreted by clients with a diverse set backgrounds
- Collaborated with sales during client meetings, represented ProCircular at conferences, and conducted demonstrations with potential clients to improve relationships which ultimately led to multiple SLAs being signed

Open Source Projects:

Typescript

- implemented xchacha20poly1305 in typescript available on github under the stablelib repository

Rust

- Led development in Indy-SDK to easily encrypt, sign, decrypt and verify messages while retaining provenance of the message using the JWE and JWS standards
- Assisted development of libsovtoken plugin for Indy-SDK which enabled payment functionality for use with Indy Plenum token plugin

Python

- Contributed nearly 5,000 lines of tests and refactors to the development of a token plugin for Indy Plenum
- Made a python3 client API to communicate with the DIF universal resolver to resolve DIDs from blockchains

Java

- Built a password manager using AES encryption and SHA512 hashing with open-source libraries
- Implemented a one-time-pad encryption scheme and RC4 stream cipher scheme in a graduate cryptography class

Other projects

- Researched and drafted a framework used to quantify and compare a variety of identity systems
- Co-Authored a paper at Rebooting Web of Trust analyzing the different implementations of decentralized identifier authentication and authorization protocols
- Researched and provided recommendations for cryptocurrency token economic incentive models during the initial token development work at Evernym

Standards Development

- W3C Decentralized Identifiers working group, MATTR representative and implementer
- W3C Verifiable Credentials Working Group, MATTR representative and editor
- IETF draft-denhartog-pairing-curves-jose-cose-00, author
- IETF draft-looker-jwm-01, reviewer
- Various additional W3C CCG work items
- Decentralized Identity Foundation Sidetree WG, MATTR representative and contributor
- Open ID Connect SIOP V2, early contributor (while at DIF)

Group Affiliations:

W3C Verifiable Credentials working group, Editor (v1.1)	May 2021 - Present
Decentralized Identity Foundation, Technical Steering Committee member	November 2017 - Present
Hyperledger Global Forum, Indy Agent Speaker	December 2018
Hyperledger, Technical Ambassador	June 2018 - March 2020
Decentralized Identity Foundation, DID-Auth WG Chair	November 2017 - Present

Education:

University of Iowa, Iowa City, IA May 2017
Bachelor of Arts in Computer Science