Cybersecurity Pioneer Introduces Zero-Trust Data Privacy Solution in New Whitepaper

NASHVILLE, TN, USA, April 11, 2023 /EINPresswire.com/ -- Self-protecting data leader Sertainty has published a new whitepaper titled Quantum Computer Threats Against PKI Data Security and a Digital-ID Based Self-Protecting-Data Solution. The new white paper details a zero-trust data privacy solution in response to the emerging quantum computer threats against Public Key Infrastructure (PKI) data security vulnerabilities.

Cybersecurity Pioneer Introduces Novel Zero-Trust Quantum PKI Threat Solution in New Whitepaper

In the new whitepaper, Sertainty Leadership Advisor and Chief Technology Officer Dr. Behzad Nadji lays out the framework for a revolutionary solution to one of the most prominent and unresolved weaknesses in Public/Private Key Infrastructure.

Dr. Nadji received his Ph.D. in Electrical/Computer Engineering from the University of Southern California. Before joining Sertainty, he served as Senior Vice President at AT&T, and led the AT&T network design, development, and architecture team for the entire AT&T network. Dr. Nadji also served as the head of one of the most prestigious R&D Labs in the world, AT&T Bell Laboratories Research. Additionally, he holds over ten patents in various areas of technology.

PKI is a technology that uses a pair of cryptographic keys, consisting of a public key and a private key, to encrypt and decrypt data and authenticate users. PKI is a common component of cybersecurity, and it enables safe communication and transactions between parties and supports digital identity and access management. Today, Public/Private Key Infrastructure is the most commonly used technology for secure communication on the Internet.

In the whitepaper, Dr. Nadji also addresses common misconceptions about the capabilities of blockchain technology in cybersecurity and presents potential solutions that can be incorporated into existing frameworks to solve the issues posed, like Grid-based Cryptography.

Based on the industry-leading Sertainty Software Development Kit (SDK), the proposed solution utilizes self-protecting digital IDs (otherwise, Sertainty IDs or SIDs.) These SIDs are built upon a

zero-trust data privacy framework. This framework comprehensively addresses the threats resulting from current and future PKI vulnerabilities.

“When we think of creating real solutions to quantum computing threats, we need to look beyond simply ‘plugging the holes’ that can be identified in existing security systems,” says Dr. Nadji. “Quantum computing threats are fundamentally different from traditional data security vulnerabilities, and therefore require a more comprehensive approach.”

Sertainty zero-trust data privacy technology is already used in various applications, from financial technology and infrastructure projects to national intelligence operations.

About Sertainty
A leader in zero-trust data privacy and self-protecting data, Sertainty provides companies in a wide range of industries with data tracking, compliance, security, and governance with their Sertainty Data Privacy Platform. The company is also known as a thought leader in cybersecurity, having established partnerships with other industry pioneers and providing consulting services for the United States Department of Defense through Sertainty Federal Systems.

Learn more at https://sertainty.com/.

Alli
Ehrhardt
+1 541-973-1994
email us here