Otoritas Sertifikat Elektronik Berbasiskan Blockchain Dalam Implementasi Short-Lived Certificate = Blockchain Based Certificate Authority in Short-Lived Certificate Implementation

Thio Lutfi Habibi, author

Abstrak

Kegagalan revokasi sertifikat pada insiden kebocoran sertifikat pada Otoritas Sertifikat (CA), disebabkan oleh kurang efektifnya metode dan performa sistem revokasi yang diimplementasikan oleh CA. Hal ini mendasari pengembangan Short-Lived Certificate, dimana sertifikat memiliki masa validitas yang lebih singkat untuk meningkatkan aspek Computationally Secure. Inisiasi ini tidak disambut dengan begitu baik, Short-Lived Certificate menyebabkan siklus hidup sertifikat menjadi sangat cepat dan meningkatkan beban komputasi untuk penerbitan dan revokasi sertifikat pada CA. Otoritas Sertifikat Elektronik Berbasiskan Blockchain dalam penelitian ini, bertujuan untuk melakukan segregasi fungsi proses serta mendelegasikan beban penerbitan dan revokasi sertifikat digital kepada pemilik sertifikat. Metode ini diimplementasikan dengan merubah CA menjadi sistem terdistribusi dan memanfaatkan Blockchain sebagai penyimpanan terdistribusi untuk konsistensi data. Dari hasil pengujian beban transaksi pada Blockchain dengan menggunakan Hyperledger Caliper, untuk 250 node transaksi menunjukan throughput sebesar 916,7 transaksi dalam 60 detik serta 100% transaksi sukses sebesar 58.932 dengan rerata latensi transaksi 0,40 detik. Pada kondisi 300 node transaksi menunjukkan adanya 1,44% transaksi gagal dengan total transaksi 59.061 dan peningkatan rerata latensi yaitu 2,12 detik, kegagalan transaksi disebabkan oleh kondisi antrian transaksi yang tidak bisa diselesaikan dalam 60 detik. Berdasarkan pengujian tersebut disimpulkan, implementasi sistem server tunggal Otoritas Sertifikat Elektronik Berbasiskan Blockchain efektif untuk otomasi terhadap 250 sistem dengan total throughput 916,7 transaksi dalam 60 detik. Perubahan fundamental arsitektur dari sistem CA memiliki kesesuaian dengan standar RFC 3647 dan memberikan nilai tambah Computationally Secure melalui Short-Lived Certificate, sehingga dimungkinkan dilakukan pengembangan lebih lanjut untuk membangun sistem ini secara komprehensif.
.....Certificate Revocation were failure in certificate leakage incidents at Certificate Authorities (CAs), caused by ineffective methods and performance of revocation system implemented by CAs. This underlies the development of Short-Lived Certificates, where certificates have a shorter validity period to improve aspects of Computationally Secure. This initiation was not very welcome, Short-Lived Certificates caused the certificate lifecycle to be quick and increased the computational load for certificate issuance and revocation on the CA. The Blockchain-Based Electronic Certificate Authority in this study, aims to segregate process functions and delegate the burden of issuing and revoking digital certificates to certificate owners. This method is implemented by converting CA into a distributed system and utilizing Blockchain as distributed storage for data consistency. From the results of transaction load testing on the Blockchain using Hyperledger Caliper, for 250 transaction nodes showed a throughput of 916.7 transactions in 60 seconds and 100% successful transactions of 58,932 with an average transaction latency of 0.40 seconds. In the condition of 300 transaction nodes showed that 1.44% of transactions failed with a total of 59,061 transactions and an increase in average latency of 2.12 seconds, transaction failures were caused by transaction queue conditions that could not be completed in 60 seconds. Based on these tests, the implementation of Single Server System

a Blockchain-Based Electronic Certificate Authority is effective for automation of 250 systems with a total throughput of 916.7 transactions in 60 seconds. The fundamental architectural changes of the CA system are compliant with RFC 3647 standards and provide added value Computationally Secure through a Short-Lived Certificate, making it possible to further develop to build this system comprehensively.