Desain dan Implementasi Protokol Untuk Mendukung Proxy Signature = Protocol Design and Implementation to Support Proxy Signature

Nasywa Nur Fathiyah, author

Abstrak

Implementasi protokol untuk mengakomodasi proxy sign berangkat dari kekhawatiran akan keamanan penyedia tanda tangan yang memakai skema digital signature biasa. Pada skema proxy signature, original signer mendelegasikan otoritasnya kepada proxy signer tanpa mengirimkan kunci privat dari original signer (Mambo, et. al, 1994). Pada skema proxy signature, terdapat kebutuhan untuk membuat beberapa komponen pada sisi client yang sulit untuk dilakukan oleh orang awam. Maka dari itu, tujuan dari penelitian ini adalah untuk merancang dan mengimplementasi protokol yang dapat memfasilitasi proxy signature. Requirement utama dari penelitian ini adalah untuk membuat server dapat menandatangani suatu dokumen atas nama pengguna tanpa menggunakan kunci privat pengguna. Pada penelitian ini, dilakukan pengujian eksekusi protokol dan kemungkinan keadaan komponen yang diperlukan untuk membuat tanda tangan digital menggunakan skema proxy signature seperti tanggal kadaluwarsa sertifikat publik original signer, sertifikat publik proxy signer, dan input pengguna. Hasil pengujian kebenaran protokol menunjukkan bahwa protokol yang dibuat dapat mengakomodasi requirement. Hasil pengujian waktu menunjukkan bahwa proses sign memakan waktu 900 milisecond-2000 milisecond dengan 37%-52% dari waktu tersebut digunakan untuk membuat sign dengan method yang dibuat diluar penelitian ini.

.....Digital signature provider systems in Indonesia are using the regular digital signature scheme which needs private key, public key, and the document to be signed, means, these providers always hold the user’s private key which can cause security issue when the system compromised.. On proxy signature scheme, the original signer delegates its signing power to a proxy signer with some kind of warrant, without sending secret informations like original’s signer private key (Mambo, et. al, 1994). Original signer and proxy signer interacts with each other only with public information like public key. However, to sign with proxy signature scheme, user needs a protocol. The purpose of the research is to design and implement a protocol to facilitate proxy signature that is made based on the scheme that was made by Shao (2009). At the evaluation, it revealed that the protocol fulfilled the requirement and can be used to facilitate proxy signature. The execution time of the sign took 900 millisecond to 2000 millisecond with 37%-52% of the total time used to generate the sign by using the method that was made outside the scope of the research.