Penerapan Infrastruktur Kunci Publik sebagai Upaya Meningkatkan Jaminan Sekuriti dalam Transaksi Online: Studi Kasus PT Telkom sebagai Certification Authority (CA)

Buana Jaya, author

Abstrak

ABSTRAK
Seiring dengan berkembangnya sistem komputer yang terhubung melalui jaringan internet dan semakin meningkatnya individu maupun organisasi yang memiliki ketergantungan untuk mendapatkan informasi dan melakukan komunikasi melalui internet, menjadikan isu sekuriti sebagai hal yang perlu mendapatkan perhatian khusus. Salah satu pemanfaatan internet adalah e-commerce yang secara luas digunakan untuk menggantikan model perdagangan tradisional saat ini.

Dalam e-commerce dibutuhkan jaminan akan kerahasiaan informasi yang dikirimkan (confidentiality), keutuhan dan keaslian informasi (integrity), keabsahan pengiriman informasi (authentication) dan pengakuan terhadap informasi yang dikirim sehingga tidak dapat disangkal (non repudiation) merupakan syarat mutlak yang harus dipenuhi.

Teknologi saat ini yang dapat memenuhi aspek sekuriti diatas adalah Infrastruktur Kunci Publik yang menggunakan sepasang kunci yaitu kunci pribadi (private key) dan kunci publik (public key) dalam melakukan proses enkripsi dan dekripsi suatu pesan (message). Kunci publik yang dimiliki dapat diketahui oleh setiap orang yang membutuhkan dalam jaringan komunikasi. Sedangkan kunci pribadi hanya diketahui dan disimpan oleh pemilik kunci itu sendiri.

PT. Telkom sebagai salah satu penyedia layanan jasa telekomunikasi di Indonesia berupaya menjadi pihak ketiga (third party) yang menjamin kebutuhan pengguna internet terhadap pertukaran informasi. Dengan membuat layanan yang disebut I-Trust untuk Infrastruktur Kunci Publik menjadikan PT. Telkom sebagai CA (Certification Authority) yang menandatangani secara elektronik sertifikat digital. Untuk proses identifikasi dan otentifikasi terhadap subcriber (user) dari sertifikat digital yang diberikan wewenang oleh CA, PT. Telkom bekerja sarna dengan perusahaan atau organisasi menjadi Registration Authority (RA).

Pada penulisan tesis ini bertujuan untuk menerapkan infrastruktur kunci publik pada suatu perusahaan e-commerce (PT. X) sebagai Registration Authority (RA) untuk meningkatkan competitive advantage dan menciptakan entry barrier terhadap kompetitor dan dilakukan analisa kunci keberhasilan penerapan infrastruktur kunci publik.

Untuk analisa sistem sekuriti jaringan menggunakan tahapan yang ada pada Security Policy Development Life Cycle (SPDLC) dan untuk analisa kondisi eksternal perusahaan dilakukan menggunakan Competitive Force Model (Porter).
<hr>

ABSTRACT
The explosive growth in computer systems and their interconnections via internet has increased the dependence of both organizations and individuals of the information stored and communicated using this system. This in turn has led to a heightened awareness of the security issue. E-commerce is one of the most popular business model using the internet infrastructure.

In e-commerce, the widespread use of this systems, need more assurance to ensure only intended recipient are able to read the information (confidentiality), to guarantee the information was not altered during transmission (integrity), to validate the information by sender (authenticity), and to prevent the sender from denying involvement in that information (non- repudiation).

One of the technology that can fulfill all of security requirements mentioned above is Public Key Infrastructure that using a pair of key, public key and private key. These keys are used in encryption and decryption process of a massage. Anything encoded with one key can only be decoded by it's counterpart. Each user keeps one key secret and publishes the other.

PT Telkom as one of the telecommunication provider in Indonesia, is trying to become the third party to ensure this information exchange by deploying the I-TRUST service for Public Key Infrastructure. This has made PT Telkom as CA (Certification Authority) whose signed digital certificate electronically. PT Telkom as CA, has to coordinate with other party as its Registration Authority (RA) to do the identification and authentication of the subscriber's digital certificate.

The objective of this thesis is to show the implementation of public key infrastructure on an e-commerce company as Registration Authority (RA) to improve it's competitive advantage and create entry barrier to it's competitor, and analyze the key success of implementation of public key infrastructure.

Security Policy Development Life Cycle method is used to analyze network security system and Competitive Force Model (Porter) is used to analyze external condition of the company.