ABSTRACT

The most important aspect that has to be paid attantion on e-payment services is the security level of that services. With a lot of data transfer that happened on that services, some information data became most likely be vurnerable toward some attack form some unauthorized parties. The other problem is that, how would the user as well as the bank server knows that the identity that entering their system is a valid user. In other word, the authentificities of the data transmitted on the e-payment service became a factor that decides the outcome of the transaction between both parties.

The current securities procedures always using password as the authentification procedures on the e-payment transcation, for example if a user want to login on an e-payment or banking server, users have to enter their PIN (personal Identification Number) as their password. But, if the password/PIN always the same (static password) and the user continuesly re-entering the PIN, then it makes it most likely an easy mark for carders and sniffers to obtain those PIN.

This program has yet to reach the perfection, because theres still a bug that could be found at the main program, and this particular bug is the biggest obstackle that render this project failure because its shaking the very foundation of Rijndael Algorithm, which could only process 8 bits on each column of the state array. Because of there's a limitation on Java Programming Library which do not support the calculation of checksum and carry, so the exclusive library is needed. That's why this project can't be finished.

Key words: Personal Identification Number, One-Time Password, AES 128 dan Carding