Abstract

Smart Cards are currently being implemented in a system to help humans develop technology, one of which is access barriers such as identity cards as a closed door lock. Various types of cards used are divided based on the way of data communication, namely contact cards, and contactless cards, as well as various authentication methods applied. However the card used still allows duplication without the owner's knowledge. The causes of duplication are very diverse, ranging from cards that have no security at all to cards that already have security methods such as card data encryption. Therefore this study implements the Synchronized Secret method through mutual authentication, which every time the card authentication process against the card reader must authenticate each other. At each session authentication requires transaction history data in the form of random data that is always changing and cannot be known by anyone. The entire authentication process will run if the applet is installed as a communication medium. The results of several test scenarios show that the data on the card cannot be illegally read, so the card cannot be duplicated. Time process tapping requires an average of 4 seconds, so that it can be an alternative to the authentication process that existed before.

Keywords: ***smart card, mutual authentication, applet, synchronized secret.***