IMPLEMENTATION OF DATA SHARING SECURITY USING PRETTY GOOD PRIVACY (PGP) AND BASE64 ON MOBILE APPLICATION

DICKY CAHYO NUGROHO
(Pembimbing : Heru Agus Santoso, Ph.D)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201307632@mhs.dinus.ac.id

ABSTRAK

Pretty Good Privacy (PGP), a security infrastructure developed by Phil Zimmermann in mid-1980 that allows a person-to-person exchange of information via the internet by providing confidential protection against man-in-the-middle risks in forms of encryption/decryption and authentication using digitally signature. PGP uses symmetrical and public/private key cryptography in two levels: the secret key (symmetric), also called the session key, to perform data encryption and private/public key to provide and protect symmetric keys. The main functions of the PGP among others to perform encryption and create a digital signature on files, decrypt and verify files that have digital signatures, and manage PGP keys collection owned. The purpose of PGP is to provide and protect three main elements:, first, privacy, confidentiality in the storage and transmission of data to be secured so that only people who can access it, second, integrity, security against data from being modified without the knowledge of the owner, and the third, authentication, guarantee ownership of the data. In this work report we study about how to implement PGP into data sharing, how to make our data secure when it is sent into receiver. And also it can be use practically.

Kata Kunci : PGP protocol, middle attacks,mobile application

IMPLEMENTATION OF DATA SHARING SECURITY USING PRETTY GOOD PRIVACY (PGP) AND BASE64 ON MOBILE APPLICATION

DICKY CAHYO NUGROHO
(Lecturer : Heru Agus Santoso, Ph.D)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201307632@mhs.dinus.ac.id

ABSTRACT

Pretty Good Privacy (PGP), a security infrastructure developed by Phil Zimmermann in mid-1980 that allows a person-to-person exchange of information via the internet by providing confidential protection against man-in-the-middle risks in forms of encryption/decryption and authentication using digitally signature. PGP uses symmetrical and public/private key cryptography in two levels: the secret key (symmetric), also called the session key, to perform data encryption and private/public key to provide and protect symmetric keys. The main functions of the PGP among others to perform encryption and create a digital signature on files, decrypt and verify files that have digital signatures, and manage PGP keys collection owned. The purpose of PGP is to provide and protect three main elements:, first, privacy, confidentiality in the storage and transmission of data to be secured so that only people who can access it, second, integrity, security against data from being modified without the knowledge of the owner, and the third, authentication, guarantee ownership of the data. In this work report we study about how to implement PGP into data sharing, how to make our data secure when it is sent into receiver. And also it can be use practically.

Keyword : PGP protocol, middle attacks, mobile Application