Using DES-1551 Module (SEM-4030)

Using DES-1551 Module (SEM-4030)

Electronic mail (Email) is one of the most popular Internet services. People using thisservice is able to send Emails to everywhere in the world with a low cost. Emails in the way from source to destination and also when they are stored on the server can be seen, deleted or even forged. To prevent these threats in the Email service the Public Key Infrastructure (PKI) is utilized.

This infrastructure is supported by most Email clients such as Netscape, Mozilla Thunderbird and Microsoft Outlook. In this method the Email is first encrypted by the receiver's public key and then is signed by sender's private key.

In the receiver's side the signature is verified by sender's public key and then it is decrypted by receiver's private key. So confidentiality and integrity of Emails are achieved by this method. In this infrastructure, public key of every individual is certified by a Certificate Authority (CA) and is published as a digital certificate. The private key must be kept secure and protected. Secure tokens are the most helpful devices to store private keys securely. Also Email clients such as Netscape and Mozilla Thunderbird, Supporting the PKCS#11 standard, can use the private keys stored in compatible secure tokens.

DES-1551module (model W) as a secure token supports PKCS#11 standard and it can be used in Usual Email client softwares and protect user's private key.

DES-1551Certilicate Manager software is designed to manage certificates and private keys stored on DES-1551 Using this software private keys and digital certificates can be imported into DES-1551 memory using pl2 files which are based on PKCS#12 standard.

Technical Specifications:

- Certificate and private key management software (DES-I55I Certificate Manager)
- Secure storage of private keys
- X.509-based storage of digital certificates in DES.1551 module
- Lack of unauthorized access to user's sensitive information
- User authentication while accessing DES-1551 module by a PIN
- Certificate and private key management (using pl2 files which are based on PKCS# 12 standard)
- Storage of multiple certificates and private keys in one DES-1551 module.

Forging ahead daily
Web Site: www.ieimil.ir
E-mail: marketing@ieicorp.ir