Digital Signatures In E-Business

The open nature of the Internet makes the interception of messages a relatively easy task and this in turn causes a problem for people and organizations wishing to exchange information that is either private or confidential in nature. While cryptosystems have existed in various forms throughout the ages benefiting mainly military and financial applications, they have recently taken on a more prominent role in the application of digital signatures in e-business.

There are two main types of cryptosystems. In symmetric systems, the encryption and decryption keys are identical and therefore must be kept secret. By contrast, an asymmetric system uses two sets of different keys one for encryption, which is a *public key*, and the other for decryption, which is a *private key*. Asymmetric systems provide the basis for digital signatures in e-business. A third party referred to as a Certification Authority, is also necessary to register, authenticate and manage keys and users. This whole process, sometimes referred to as Public Key Infrastructure (or PKI) assures the following:

- A message that is encrypted using the public key can only be decrypted by using the private key. This is ensures that if the message is intercepted, no one can deduce its content except the owner of the private key.

- A message that is encrypted by the secret key can only be decrypted by using the public key. This in turn ensures the authenticity of the sender.

This brings us to the point of having our own independent Certification Authority in Jordan. The establishment of such an authority, which is a basic requirement for e-business not to mention e-government, has been the topic of numerous reports, presentations, discussions, recommendations as well as policy and strategy papers during the past three years. It is long overdue and about time that it comes into existence.