DIGITAL CERTIFICATES

The e-Procurement System that is being implemented to handle procurement processes is integrated with ‘state of the art’ security to manage the confidentiality and integrity of bid data. This has been achieved through the unique and internationally patented Secure Bid Process offered by Nextenders – the solution provider of e-Procurement System.

To manage the security and integrity of bid data that is processed using the e-Procurement System, it is mandatory for the Suppliers to obtain a digital certificate. Some common clarifications on digital certificate are provided as below:

Q. What is Public Key Infrastructure?
A. A Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority. For more information on PKI, please see – http://en.wikipedia.org/wiki/Public-key_infrastructure.

Q. What is a digital certificate?
A. In simple terms, a digital certificate is an equivalent of a human signature in the digital world. Like an individual is bound to a physical document by his / her signature, in the digital world, this can be established through the use of digital certificate.

A digital certificate is a unique combination of a public key and a private key that is used to encrypt and to digitally sign electronic data in the Systems / Forms that are designed to allow encryption and digital signing. The data encrypted by the public key can be decrypted only using the matching private key and vice versa. For more information on digital certificates, please see - http://en.wikipedia.org/wiki/Digital_certificate.

Q. What is the use of digital certificate on the e-Procurement System?
A. Digital certificate will be used to encrypt and sign the bid data prepared by the Suppliers on the e-Procurement System. It is mandatory for all Suppliers to encrypt and sign bid data before submitting it on the System. This is required to ensure the confidentiality and non-repudiation of the information
submitted on the System. The e-Procurement System is designed to ensure that all data that is submitted through the client (the computer system of the User) to the server is always transmitted and stored in encrypted form.

Q. Who can apply for a digital certificate?
A. A person who is duly authorized to represent the organization that is interested in doing business with any of the Public Bodies in Mauritius may apply for a digital certificate. There can be more than one applicant from the same organization who can apply for a digital certificate.

Q. How do I apply a digital certificate?
A. It is mandatory to apply for a digital certificate that is issued by a licensed Certifying Authority that is registered with the Controller of Certifying Authority of Government of Mauritius. Currently, there is one Certifying Authority that is registered and licensed to issue digital certificates, which is eMudhra Consumer Services Limited (www.emudhra.mu).

Q. How do I store a digital certificate?
A. A digital certificate is to be stored very securely and in sole possession of the applicant in whose name it has been issued. Any transaction that is signed by the digital certificate (whether authorized or unauthorized) binds the applicant in whose name it has been issued, unless the digital certificate has expired or has been revoked (process by which the validity of the digital certificate is forcefully cancelled). At any point in time after the issuance of digital certificate, if the applicant feels that the control of the digital certificate has been compromised for any reason whatsoever, the applicant is required to immediately initiate the process of revocation of the digital certificate.

For any further information on digital certificates, you may contact the Helpdesk Support Team.