Land Titles (Electronic Lodgment) Rules 2003

Table of Contents

No. S 275

LAND TITLES ACT
(CHAPTER 157)

LAND TITLES (ELECTRONIC LODGMENT) RULES 2003

In exercise of the powers conferred by section 170(1A) of the Land Titles Act, the Singapore Land Authority hereby makes the following Rules:

Citation and commencement

1. These Rules may be cited as the Land Titles (Electronic Lodgment) Rules 2003 and shall come into operation on 9th June 2003.

Definitions

2. In these Rules, unless the context otherwise requires —

"approved certification authority" means any person or organisation named in the First Schedule that issues a certificate;

"asymmetric cryptosystem" means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify the digital signature;

"certificate" means a record that at a minimum —

(*a*) identifies the approved certification authority issuing it;

(*b*) names or identifies its subscriber;

(*c*) contains the subscriber's public key; and

(*d*) is digitally signed by the approved certification authority issuing it;

"correspond", in relation to private or public keys, means to belong to the same key pair;

"digital signature" means an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine —

(*a*) whether the transformation was created using the private key that corresponds to the signer's public key; and

(*b*) whether the initial electronic record has been altered since the

transformation was made;

"electronic record" means a record generated, communicated, received or stored by any electronic, magnetic, optical or other means of storage in an information system or for transmission from one information system to another;

"electronic signature" means any letter, character, number or other symbol in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record;

"hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller set (the hash result) such that —

(*a*) a record yields the same hash result every time the algorithm is executed using the same record as input;

(*b*) it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm; and

(*c*) it is computationally infeasible that 2 records can be found that produce the same hash result using the algorithm;

"key pair", in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates;

"private key" means the key of a key pair used to create a digital signature;

"public key" means the key of a key pair used to verify a digital signature;

"signature" includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods;

"subscriber" means a person who is the subject named or identified in a certificate issued to him by a certification authority and who holds a private key that corresponds to a public key listed in that certificate;

"verify a digital signature", in relation to a given digital signature, record and public key, means to determine accurately that —

(*a*) the digital signature was created using the private key corresponding to the public key listed in the certificate; and

(*b*) the record has not been altered since its digital signature was created.