METHOD AND SYSTEM FOR DISTRIBUTED CRYPTOGRAPHIC KEY PROVISIONING AND STORAGE VIA ELLIPTIC CURVE CRYPTOGRAPHY

ABSTRACT OF THE DISCLOSURE

A method for distributing multiple cryptographic keys used to access data includes: receiving a data signal superimposed with an access key request, wherein the access key request includes at least a number, n, greater than 1, of requested keys; generating n key pairs using a key pair generation algorithm, wherein each key pair includes a private key and a public key; deriving an access private key by applying the private key included in each of the n key pairs to a key derivation algorithm; generating an access public key corresponding to the derived access private key using the key pair generation algorithm; and electronically transmitting a data signal superimposed with a private key included in one of the n key pairs for each of the n key pairs.

FIG. 1