# AUTOKEY INITIALIZATION OF CRYPTOGRAPHIC DEVICES


## ABSTRACT OF THE DISCLOSURE

In a cryptographic system, a device is manufactured with a secure section that generates an internal secret. An irreversible cryptographic transform of the internal secret is created and a certificate containing the irreversible cryptographic transform and a unique identifier of the device is signed using a manufacturer key. The device and the certificate are provided to a network operator. An initialization process is performed under the control of the operator to set up a secure channel between two devices under the control of the operator for secure communications between the two devices. Because of the internal secrets maintained within each device and the certificates, the devices can authenticate each other and communicate securely, even over an insecure channel, without needing the devices to have been previously programmed with a secret of the operator. The devices can authenticate each other and create a shared secret, all over an insecure channel.

(Fig. 1)