

162162

METHOD AND APPARATUS FOR INITIALIZING SECURE COMMUNICATIONS AMONG, AND FOR EXCLUSIVELY PAIRING WIRELESS DEVICES

ABSTRACT

A method for establishing a security relationship between a first device and a second device, said first and second devices each having an associated device certificate, each of said device certificates having a unique device identifier for said corresponding device, said method comprising the steps of initiating a pairing request one of said devices to the other of said devices; sending, from said first device, the device certificate of said first device to said second device; cryptographically verifying, by said second device, said received device certificate of said first device; outputting, at said second device, the device identifier of said first device contained in said first device certificate; verifying, by said user, that said output device identifier matches the unique identifier of said first device, said unique identifier being known to said user; and, accepting, by said user, the association of said first device and said second device if said displayed device identifier is verified.

FIG. 4

