

SYSTEM AND METHOD FOR MANAGING SECURE COMMUNICATIONS BETWEEN MODULES IN A CONTROLLER AREA NETWORK

ABSTRACT

This document describes a system and method for managing communications between modules in a Controller Area Network (CAN) in a secure manner. In particular, the system employs a hierarchical key generation method that allows a module in the CAN to use a single ascendant key together with relevant identifiers to generate descendant keys for CAN identities in the Controller Area Network. These keys are then used by the broadcasting and receiving CAN modules to authenticate published messages.

Figure 1