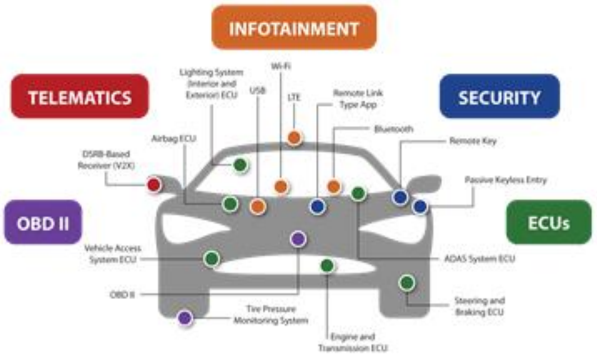
ANGOKA

Enabling New Automotive Applications

ANGOKA is a UK-based cybersecurity start-up, and has already compiled an enviable list of collaborators and customers, such as BT and Innovate UK. They recognise that ANGOKA's technology for authenticating communications between electronic devices can radically improve machine-to-machine (M2M) cybersecurity.

- Higher level of security
  - Our solution is based on hardware
  - Intrinsically safer than relying on software alone
- Cost-effective
  - Hardware collaboratively creates passwords in real-time
  - Removes need to periodically upload new passwords
- Widely applicable
  - Provides trusted communications in an untrusted network
  - Can be used across all types of vehicles



Device Authentication Unit

The heart of ANGOKA's system is a Device Authentication Unit (DAU) – a hardware unit that is small enough to be fitted within a chip.

On start-up, each device contributes a part of a session key – a unique password shared between authorised devices on the network. The client decides on the refresh frequency of the session key during the configuration phase: on a vehicle, for example, that could be every time it is started.

New Market Opportunities

The fact that the system creates its own keys, and needs no updating, opens up new market opportunities for automotive clients. These are both safety-critical applications, where the highest possible security standards are needed, and also low-cost applications, which cannot justify the cost of subscription-based third-party certification services.

Safety-critical: A typical use-case would be teleoperation of autonomous vehicles (e.g. goods vehicles in logistics hubs or passenger shuttles in city centres). Because the vehicles only have to talk to each other and to their operator, every link in the communications chain can be protected by ANGOKA DAUs.

Low cost: ANGOKA's solution makes secure asset condition monitoring (e.g. continuous monitoring of an electric motor or a battery) feasible. Again, with the asset only communicating with its manufacturer (either the OEM or Tier One), the necessary security becomes highly cost-effective.