Low-power, secure AES-128-based transponder intended for car key fob applications

Atmel announced the availability of a new secure, ultra-low-power micromodule transponder based on an Atmel AVR microcontroller (MCU). Used for remote keyless entry systems in vehicles, the ATA5580 transponder includes the Atmel open immobilizer protocol stack with a built-in, high-performance AES-128 hardware cryptographic unit, a low-frequency (LF) immobilizer interface for power supply and bi-directional communication, and an LF antenna. The ATA5580 standalone immobilizer transponder is intended to be over-molded in simple mechanical keys which are usually accompanying full featured remote keyless entry key fobs. For this purpose, the ATA5580 immobilizer transponder and the ATA5795 remote keyless entry AVR microcontroller feature the same LF, protocol and AES implementations allowing seamless deployment of both types of keys in a single system.

Based on a land grid array- (LGA-) like package, the ATA5580 transponder avoids usage of a lead frame construction providing best-in-class electrostatic discharge (ESD) protection that is especially important in harsh environments such as over-molding processes.

The ultra-low power design along with the high modulation index delivers a typical coupling factor in the range of 1% while running a complete AES authentication. Since typical AES immobilizer transponders exhibit significantly higher coupling factor requirements, the ATA5580 is unique in allowing car manufacturers to transition from deprecated cryptographic systems to AES without the necessity for expensive lock cylinder mechanical redesigns.

The AVR microcontroller embeds 8kB Flash and 2kB EEPROM memory hosting the Atmel open immobilizer software stack programmed during manufacturing. The protocol stack, released under an open source license allows true peer-reviewing process and security audits.

Finally, while all traditional competitive offering has a one-size-fits-all approach, the ATA5580’s immobilizer protocol is made heavily configurable via EEPROM allowing designers to easily optimize system parameters such as authentication time against coupling factor/bit security, maximizing the communication link robustness for a given environment.

“Immobilizer systems are the most critical function of a car access system. They are simply not allowed to fail. The ATA5580 offers a particularly attractive combination of high-security AES cryptography along with coupling factor requirements usually found in basic transponder state-machines featuring insecure immobilizer algorithms. This device proves that AES does not mean high power consumption,” said Dr. Jedidi Kamouaa, marketing manager for car access products, Atmel

Corporation.

Availability and pricing
Samples of the ATA5580 are now available. Pricing starts at USD $2.00 for 10,000-piece quantities. The ATA5580 immobilizer transponder along with the ATA5795 remote keyless entry AVR microcontroller are supported by the new ATAK51001 evaluation kit providing hardware and software reference design for complete car access application developments.

For details, visit www.atmel.com [1]

Source URL (retrieved on *09/30/2014 - 9:02am*):
http://www.ecnmag.com/product-releases/2012/04/low-power-secure-aes-128-based-transponder-intended-car-key-fob-applications

Links:
[1] https://webmailus2.atmel.com/OWA/redir.aspx?C=cb68f14298694c20aa05109b70b79c0d&URL=http%3a%2f%2fwww.atmel.com%2fMicrosite%2ftechlive2012%2fdefault.aspx