Designing Next-Generation Key Fobs

Paul Lepek

Key Fobs Today

Today's key fobs can be generally subdivided into two different functional categories. The first includes Remote Keyless Entry (RKE) devices which require some sort of human intervention or a physical interface of the user to the key fob (e.g., key push) in order for the fob to produce the desired function effect such as unlocking a door or opening a sunroof. The second group of devices provides similar functionality but also features an added level of comfort by performing the same function without physical intervention by the user. Instead of the push button or touch sensor interface, a Passive Entry (PE) identifies the user (and the key fob) as a legitimate entity and automatically triggers authentication or issues a request (e.g., passive door unlock, trunk release, etc.).

Both systems are based on a preprogrammed key fob device ID and authentication protocols which include an encryption stage for authorizing the issue of key fob commands to the vehicle. In this way the key can be identified by the vehicle and vice versa before any action is executed. All RKE-based systems require key fobs to support RF links which fall into Industrial, Scientific and Medical (ISM) frequency bands (i.e., 0 - 135kHz, 13.56MHz, 315/433MHz, 869MHz, and 915MHz). However, for a PE system the LF downlink is used by the key fob to compute a Received Signal Strength Indicator (RSSI) value and thus the fob's physical coordinates in relation to the vehicle while the RF link is used to execute the authentication protocol with the vehicle. RKE and PE system fobs are designed to be powered by a small coin battery intended to last for the life of the vehicle.

Atmel has Introduced Next-Generation Transceiver and Receiver Devices with Configurable Options

Moreover, all key fobs support engine immobilizer system authentication. To prevent theft every automobile uses an immobilizer system which authenticates engine starts. In this case the key fob acts as a passive authentication tag similar to the RFID tag but with a larger feature set. Most automotive key fobs use Near Field Communication (NFC) transponders which communicate with the engine controller. The transponder is integrated into the key and is a passive device. It does not need a battery for operation, but instead uses a magnetic field generated by the LF vehicle coil. It also transmits the device ID and executes a special immobilizer

Table 1. Key Fob Features Today

Class	Immobilizer[1]	Batttery/ Recharge[2]	Physical Interface [3] (Button, Touch, etc.)			Passive (Entry/Go) Accessories	Personalization Settings	Time/ Data Logging in Fob[4]
			Remote Start	Remote Entry	Accessories			
Basic	x	-	-	-	-	-	x	x
RKE (std.)	x	x/	x	-	-	-	x	
RKE (ext.)	x	x/x	x	-	x	-	x	x
PE (std.)	x	x/x	x	x	x	x/x	x	
PE (ext.)	x	x/x	x	x	x	x/x	x	x

[1]Immobilizer support includes secure fob and vehicle authentication via the LF field using an integrated LF transponder.

[2]The fob includes a built-in battery with the option of recharging the battery via the LF field.

[3]Remote Start and Remote Entry are controlled via RF uni- or bi-directional link. Control of accessories can either be done using RF or IrDA links.

[4] Data can be logged such as time stamp data, last device ID, last vehicle service date, and much more either via LF or RF links.

protocol for its authentication but all communication takes place via an LF field generated by the vehicle.

Expanding Fob Applications

Originally key fobs were designed for only one purpose: to unlock the door and start the engine with the metal key. Later, RKE devices were used to remotely (HF field) unlock the door. The integrated contactless passive transponder (LF field) then unlocked the steering column and enabled the engine start.

Only more recently fobs began to penetrate convenience, general utilities, secure communications, and secure access ID applications (even extending to payment systems and e-ticketing). These functions were not developed before due to a lack of hardware and software resources, primarily because of the fob's physical size and power consumption. Recently, however, it has become possible to overcome these shortcomings by incorporating much larger user and program memories, and the use of faster, more compact, and ultra-low power processors without increasing the cost of production. Additionally, the integration of flexible, reconfigurable, and secure authentication peripherals can be made feasible. These types of peripherals include crypto units, secure key management features, and integration of smart cards useful for payment, user ID, and cipher-based authentication systems. An automotive key fob can therefore be used not only to interact with the vehicle but also to gain entry to a park garage, ski lift or to purchase train tickets. This can deliver considerable benefits when goods are purchased using one of the major credit card networks. The secure user memory can also be used to store personal and secure information as personal data ID and provide transit information for e-ticketing.

System-in-fob Hardware Resources

- Ultra-low-power 8-bit microcontroller
- Large Flash program and EEPROM data memory (memory segmentation with locks)
- RF communication interfaces
  - Infrared (IrDA) IF
  - Immobilizer IF at 125kHz
  - Passive entry IF at 125kHz (RX only)
  - Smart card IF at 13.5MHz
  - RKE IF at 315, 413, 868, 915MHz (frequency hopping)
- Power management (optional battery charge)
- Hardware cryptological unit (AES-128)
- Integrated proximity coupling smart card (ISO 14443)
- Cyclic Redundancy Check (CRC) block
- Serial interfaces (SPI, SSI)
- ISP/debug (dW)
- Analog comparator
- Flexible GP timers and WDT
- Oscillators: RTC, INTRC (125kHz, 4MHz)

The heart of a modern key is an ultra-low power microcontroller with sufficient program and data memories. Typical program memory can range from 8KB to 16KB and beyond with its data memory ranging from 1KB to 2KB depending on application requirements. Because of secure application support, the key fob's program and data memories must have provisions for memory segmentation and locks in both memory blocks. For example, the application firmware resident in program memory can be divided into separate memory sectors (e.g., application and immobilizer sections). Also data memory may have its own partitioning which can allow for soft and hard memory locks when it comes to releasing user-sensitive device-stored data (e.g., authorization password or secure key). While the microcontroller core executes application firmware, the secure user and key data is stored in the on-chip nonvolatile memories (EEPROM).

The core uses various wireless communication peripheral interfaces to communicate with the infrared transceiver (IrDA), the LF transponder (125kHz), the 3D LF receiver (125kHz), the smart card (13.5MHz) and the RKE transceiver (315, 413, 868, 915MHz). Flexible serial interfaces can be shared such as SPI or Serial Synchronous Interface (SSI) to enable data exchange with every communication peripheral. A hardware data integrity check module, based on a Cyclic Redundancy Check (CRC) checksum algorithm, supports validation of received data.

A unique feature of the immobilizer transponder interface is that it is closely bound to the power management unit which is used to provide power supply voltage, V_{DD}, while exchanging LF data with the immobilizer in passive mode. In this mode all other communication with the key fob is disabled to support batteryless operation. Some key fobs may also support the battery charge feature which is integrated into the power management module for recharging the battery with the engine running.

While in secure smart card mode the device can also operate in passive mode and exchange as well as encrypt and decrypt proprietary data using its own crypto module with the reader at F_C = 13.5MHz. It can use its own device memory or the fob's internal nonvolatile memory.

Integrated crypto modules can support many different cipher algorithms—the most popular being the 256-bit block cipher known as the Advanced Encryption Standard (AES) based on the Rijndael algorithm which can be used with a 128-bit, 196-bit or 256-bit secret key.

The fob must also contain analog peripherals such as internal oscillators where F = 125 kHz and 4 MHz to generate its internal clock signals used for the transponder front end and the microcontroller core, respectively, with low frequency deviation across VDD and temperature. The supplied analog comparator can facilitate detection of VDD drops and prevent data corruption during nonvolatile data memory writes in passive mode.

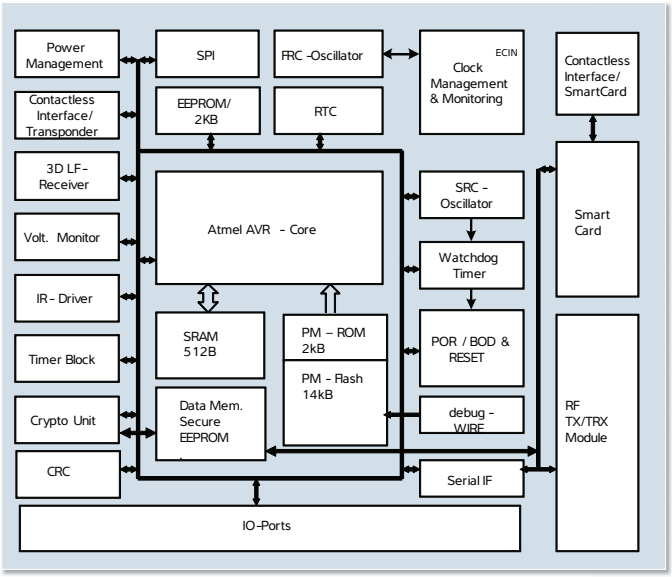

Figure 1. Fob Floor Plan

Wireless Data Communication Interfaces

An entry/immobilizer system consists of at least two communication partners where one side is on the vehicle and the other on the key fob. Depending on the link type, there are several possible communication interfaces available, including:

1. IrDA link for convenience and comfort applications
2. PE/PEG link to enter and start engine, including LF downlinks and UHF uplinks
3. Immobilizer link to start engine and emergency vehicle entry, including LF down- and uplinks
4. Chip card as user ID, authorization, authentication at pay stations, including HF down- and uplinks
5. RKE as entry authentication, including UHF down- and uplinks

Table 2. Modern Key Fob Communication Links – Overview

Application	Standard	Link Type	F_c	Modulation	Anti-collision	Data Encoding	BR [Baud]	Range	Average Current
PE/PEG	Custom	3D LF downlink	0 - 130kHz	ASK	x	PIE	3.9k	3 - 5m	2 - 20µA
		UHF uplink	315, 433, 868, 915MHz	ASK/FSK	-	Manchester, Biphase	Up to 80k	30 - 120m	8 - 20mA
Immobilizer/ Emergency Entry	ISO14223 /Custom	LF downlink	0 - 130kHz	ASK	-	PIE	3.1 -8.9k	2 - 10cm	40 - 260µA
		LF uplink		ASK		Manchester	4.4k		
Chip Card	ISO14443 ISO15693 ISO18000	HF downlink	13.56MHz	ASK/PSK	x	PIE, Miller, NRZ	Up to 20k	5 - 20cm	20 - 120µa
		HF uplink		ASK/BPSK		Manchester, NRZ			
RKE	Custom	UHF downlink	315, 433, 868, 915MHz	ASK/FSK/ PSK	x	Manchester, Biphase	Up to 80k	30 - 120m	8 - 20mA
		UHF uplink							

The summary of the communication channels and a brief overview is shown in table 2.

Secure and Reconfigurable Firmware

Application firmware which supports the complete functionality and feature set is the fundamental building block of the key fob. It may consist of many different modules and must encompass all functional and likely operating scenarios, including battery failure which comprises emergency or passive operation mode. To improve reliability it is a common practice to keep both application and immobilizer programs separate and in two distinct program spaces. While the immobilizer firmware supports distinct engine starts, the application software controls all other fob functionalities including RKE, convenience or user-ID applications. The immobilizer/emergency functionality is required to take priority over any other function, which is the equivalent of an override which suspends any function currently in progress when the LF field is detected at the transponder LF coil. Figure 2 depicts a flow diagram and interaction between application and immobilizer firmware.

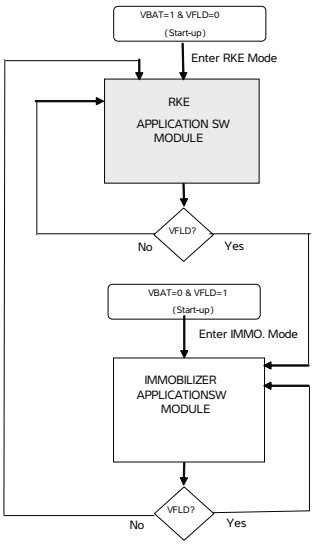

Figure 2. Immobilizer and Application Firmware Interaction Flow Chart

All data communication is fully supported in the fob's firmware. Various communication protocols including unilateral, bilateral for immobilizer, PE/PEG and RKE systems can be fully configured by the application software. Based on

protocol topology, the application software controls dedicated peripherals by enabling them, and reading data during RX phases, and writing data during TX phases of the protocol as soft triggers (e.g., immobilizer and PE applications) or hard triggers (e.g., RKE or IrDA applications using a push button interface).

A major advantage of a next-generation key fob is its in-field programmability, which can be very helpful in the event of a firmware or user data upgrade or programming. The fob can be initially configured using its dedicated general-purpose software via the LF field while the final test is performed at the factory. The user data can be added later by the Tier1 or OEM without modifying the original configuration. Even while in the field the fobs can be reprogrammed with new

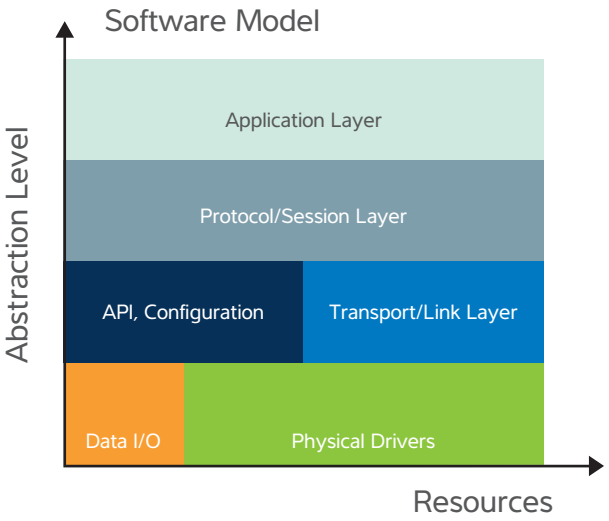

Figure 3. Software Partitioning as a Bottom-up Approach

application and user data via one of the communication interfaces at a later date. Of course, in this case only a single functionality can be enabled while using memory locks to provide security. This is especially useful when used as a pay token in e-commerce or e-ticketing environments.

Transponder LF Field Coupling

Transponder-to-base-station coupling still remains the most challenging aspect for key fobs. The proper transponder coupling can be achieved when sufficient energy is transferred from the base station to the transponder for the transponder to communicate with the base station. During design, the L-C tank must be carefully selected for optimum energy and communication performance. Figure 4 shows a typical transponder coupling at 125kHz vs. operating distance from the base station coil[5].

Coupling Factors for Immobilizer System

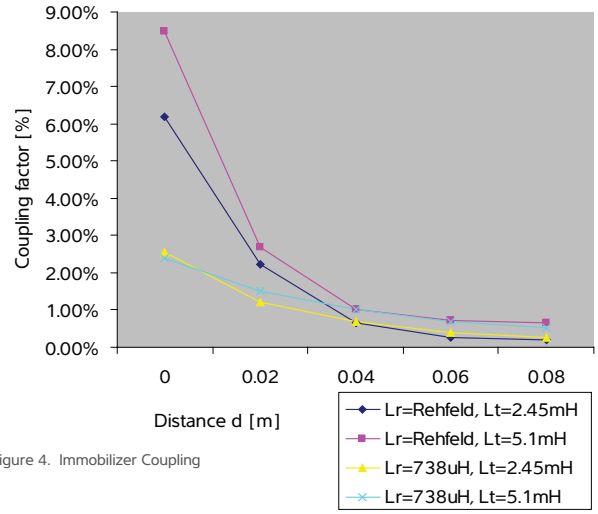

Figure 4. Immobilizer Coupling

Figure 5 shows one complete challenge-response authentication protocol which could be used in a passive automotive immobilizer application. The LF field voltage (green) is enabled for 160ms. The field is damped (2.2V) during RX state and then switched to the undamped level (6V) during TX state. The charge storage capacitor voltage (yellow) which provides V_{DD} to the transponder is immediately charged to 2.2V during the RX data stage. The transponder encrypts (AES-128) received plain text data (128-bit challenge) and transmits the response. In many immobilizer systems the system authentication time is a major concern. To minimize authentication time, the number of bits transmitted can be reduced without compromising system security. It is common for authentication time T_{AUT} < 130ms at BR = ~3.9kBaud.

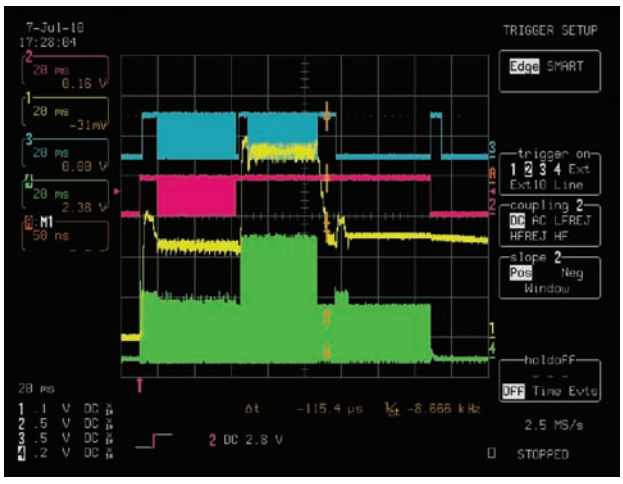

Figure 5. Immobilizer Protocol Execution Scope Shot/Power Analysis

[5] Assumes the fob coil is placed in the center of the base station coil where the coupling is best

Figure 6 shows field voltage and VCC traces as the key fob is energized by the field and begins to receive a BPLM data stream. Field gaps are visible which separate field 'On' interval which is decoded by the fob using a dedicated hardware peripheral. The fob's microcontroller is in sleep mode 95% of the time to save power consumption.

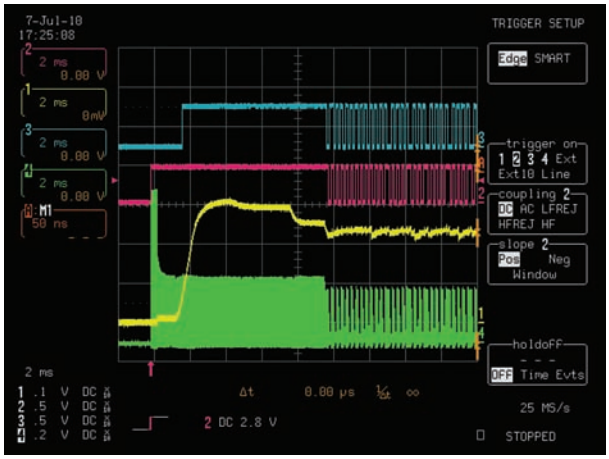

Figure 6. Transponder at Power-up

RF Communication Links

Both RKE and PE/PEG systems utilize HF communications links. In comparison to LF links, HF links are superior in their operating range (up to several hundred meters) and baud rate (up to 80kBaud can be achieved). RF transceivers currently available on the market use N-fractional PLL frequency tuning techniques where the carrier frequency can be selected in firmware by the MCU. Some devices allow large tuning frequency variations, permitting more design flexibility. The transceiver's operating range remains a key performance parameter. To extend operating range, it is common for the transmitter power to be as high as 12.5dBm and the receiver sensitivity to be less than -100dBm. Antenna design is also a determining factor providing additional performance gain. Although whip antennas add additional performance gain, small loop antennas printed on the PCB are usually chosen for use in automotive key fobs. Power consumption is another critical factor on the receiver as well as on the transmitter side. Power consumption can be reduced by selecting higher data baud rates. Choosing ASK modulation tends to lower operating current since the power amplifier is momentarily disabled during modulation.

Table 3. RF Transceiver Parameters

	Sensitivity	Antenna Gain	P_{OUT}	Average Current
Receiver	-109dBm	-6dB	-	~6 - 8mA
Transmitter	-	-18dB	10dBm	~9 - 10mA

Table 3 shows some typical RF transceiver parameters.

A snapshot of the transmitter spectrum taken at 433MHz during transmission of an RKE message to the vehicle is shown in Figure 7. The transmitter carrier frequency, the span, power output, and device setting are configured using the serial interface by shifting configuration data (in this case the 32-bit configuration word) into the RF transmitter via the MCU when the user presses the open-door button.

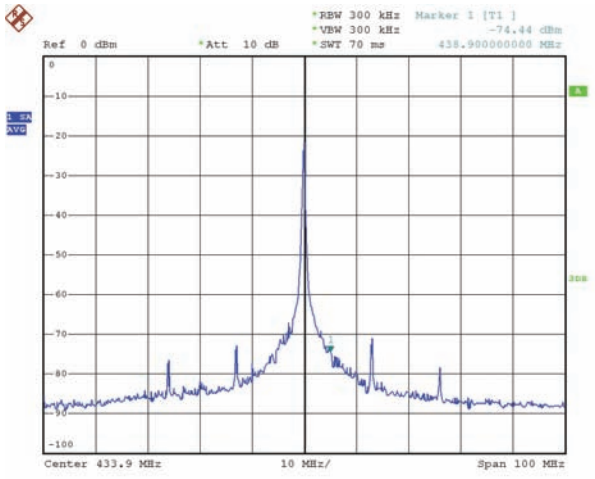

Figure 7. RF TX Spectrum at 433MHz

References:

1. ISO 14223 – Advanced Transponders Standard
2. ISO 10536 – Close Coupling Smart Cards Standard
3. ISO 14443 – Proximity Coupling Smart Cards Standard
4. ISO 15693 – Vicinity Coupling Smart Cards Standard
5. ISO 18000 – Item Management Standard