

RFID Is Key to Car Clubs' Success

Hundreds of thousands of drivers worldwide prefer car-sharing to owning their own wheels—and they use an RFID-enabled card or fob to get in the driver's seat.

By Mary Catherine O'Connor

Jan. 7, 2008—With gas prices and consumers' motivation to lessen their impact on the environment both rising, the growth of car-sharing programs is booming. Currently, approximately 348,000 individuals in 600 cities in 18 countries worldwide share nearly 11,700 vehicles as part of organized car-sharing services, according to a 2007 study by the [Transportation Sustainability Research Center](#) at the University of California, Berkeley. And nearly all of those car-sharing drivers carry an RFID card or key fob to access the cars they use. "RFID cards are the predominant means for accessing car-sharing vehicles," says Susan Shaheen, research director at the center and coauthor of the study.

Members of car-sharing programs use online schedulers to reserve cars, which are parked at set locations throughout a particular city or town. Most clubs charge hourly rates, along with a small fee per mile. The clubs offer fleets of fuel-efficient models, and many feature hybrid or electric cars. To make it easy for members to borrow any car within a fleet, the clubs send them RFID cards or key fobs when they join.

To open the door of a reserved car, a member holds the RFID card or fob up to a small dashboard-mounted computer containing an RFID reader. The interrogator collects the member's ID, encoded to the RFID tag inside the card or fob, by reading it through the car's windshield. The computer then transmits the number, via a cellular phone network, to a reservations system on a server maintained by the car-sharing company. If the system shows that the member has reserved that car, the computer unlocks the doors.

Most car-sharing clubs ask drivers to leave the keys in a designated place within the car. The keys can be left inside because the computer also controls an ignition-system lock. When the driver exits the car and uses the RFID tag to lock its doors, the ignition system becomes disabled as well. Thus, even if a thief were to force his way into a locked vehicle, he could not start it with the key inside. When the doors are unlocked with the RFID tag, so is the ignition. Some clubs request that members store the key inside the car's glove compartment, which automatically locks and which can be opened only by entering a personal ID number into a keypad inside the car.

[WhizzGo](#), a U.K.-based car-share provider, turned to German firm [Invers](#) to establish its car-access system in 2004. Invers is the largest provider of RFID-based car-access systems used by car-sharing companies, according to Dave Brook, a car-sharing consultant based in Portland, Ore., and author of the [Carsharing.US blog](#). The company embeds a passive 125 kHz Hitag RFID inlay, manufactured by [NXP Semiconductors](#), in each card. The inlay is interrogated by the Invers dashboard-mounted computer, which also controls a lock on the glove box, where WhizzGo drivers secure the car keys. The ignition system is linked with the glove compartment's lock, and the car cannot be started unless the compartment has been properly opened.

The Invers computer powers a GSM-based SIM card in the computer, enabling it to exchange data with

WhizzGo's servers. It also has a keyboard that lets WhizzGo drivers send text messages to the company's reservations personnel. Charlotte Morton, WhizzGo's managing director, says drivers often use this feature to request an extension of their allotted time with the car.

City CarShare, a nonprofit car-sharing organization founded in 2001, was the only such service operating in the San Francisco Bay area until 2006, when two large for-profit car-sharing companies, Flexcar and Zipcar, entered the market. Once City CarShare began its operations, it couldn't find an easy-to-deploy, off-the-shelf car reservations and RFID card-based car-access system, so it created its own, says Brian Kusler, who at the time was a principal at City CarShare.

Before long, the organization was spending more time developing and managing the car access and reservation system than it intended to—so much so that this was inhibiting its ability to grow and raise awareness and participation in its car-sharing offerings. Therefore, it decided to spin off its reservations and RFID system, with Kusler at the helm of the new entity, to form a company called OpenCar Networks.

OpenCar Networks' goal, outside of maintaining the City CarShare reservations and RFID car-access system, is to license the technology to other car-sharing companies, both nonprofit and for-profit, Kusler says. Car-sharing companies in Austin (Texas), Cleveland, Minneapolis, Philadelphia, and Wilmington (Delaware) presently employ the OpenCar Networks system. The fobs issued by OpenCar contain passive 125 kHz RFID tags, with an RFID interrogator built into the company's dashboard-mountable computer. The member ID encoded to each driver's tag is protected with a 40-bit encryption key, he explains, so that only an interrogator inside an OpenCar computer can access the number. That number is encrypted to prevent the member ID from being read by an unauthorized party attempting to clone a legitimate card and use it to access one of the cars.

The RFID inlays and interrogators used by the OpenCar platform are supplied by Applied Wireless ID (AWID) and were originally produced for building access systems, wherein the readers are powered by a building's electrical system. When transferring that technology to the car-share platform, Kusler says, AWID and City CarShare needed to reengineer the AWID SR-2400 interrogator to lower its power requirements so it could run off a car's battery without depleting it. City CarShare's IT director, Bryce Nesbitt, says that early on, when the company had few members and some cars in the fleet were infrequently used, these actions were not enough—drivers sometimes found that the battery inside the car they intended to drive was dead.

City CarShare is now working with AWID to further refine its reader's power requirements so that, even though drivers no longer encounter dead batteries on a frequent basis, the issue will be eliminated. Looking further into the future, he says, City CarShare—which currently has 8,500 active members and a fleet of 250 vehicles—hopes to develop a partnership with public transportation systems in the San Francisco Bay area, so that the RFID-based fare card being tested by train and bus commuters might also be employed to access City CarShare automobiles parked near transit hubs. This would require that the firm migrate to a passive 13.56 MHz inlay and install interrogators able to read both these and the already-deployed 125 kHz fobs. "We would use only the ID number encoded to the transit card to identify the user," Kusler says, "and would continue to use our existing reservations systems to handle payments for the car use."

RELATED_ARTICLES Eventually, he notes, the company hopes to offer a means for commuters to utilize cell phones equipped with RFID tags that follow the Near Field Communication (NFC) protocol to access the cars, by encoding the user's member ID to the tag inside the phone. "The XceedID XF1100 is our current choice for a multi-technology readers," says Nesbitt, "as it reads AWID, ISO 14443A and NFC."

In November 2007, Flexcar and Zipcar, the two largest car-sharing companies in North America, announced a plan to merge. As a result, Flexcar automobiles, which currently use the Invers system, will migrate to Zipcar's car-access system. Zipcar and Flexcar both issue RFID cards to drivers, who then present the cards to

readers integrated in a dashboard-mounted computer. As with most car-share formats, Zipcar uses a cellular network to link the dashboard-mounted computers to its reservation system. The company has declined to provide *RFID Journal* with further details regarding its RFID cards and interrogators.

Copyright ©2005 RFID Journal, Inc. All Rights Reserved