Inside’s Next-Gen Smart Card

Oct. 29, 2002 — Inside Contactless of Aix en Provence, France, wants to be a world leader in contactless smart cards, which use RFID technology to transfer data from a chip in the card to a point-of-sale terminal. The company has announced plans to build a next-generation smart card that will be the first to use a 16-bit RISC processor.

Today, contactless smart cards use 8-bit processors, which process data more slowly. Bruno Charrat, Inside's RFID Product Marketing Manager, says a typical 8-bit chip can process an encryption algorithm in 72 milliseconds. The company says its 16-bit chip will processes the same algorithm in 4 milliseconds.

"When we decided to create this next generation card, we had three objectives in mind," says Charrat. "We wanted it to consume very little power to boost the read range. We wanted it to process transactions much faster than existing cards, and we wanted to make the actual chip very small to keep the price low."

New smart cards based on the chip, which is still in the design phase, will be available next year. The company says the card will have a read range of 50 centimeters, or about 20 inches. The chip is about .5 millimeter square, making it about half the size of typical contactless smart card chips.

One of the factors limiting the use of contactless smart cards has been security. Today's cards typically use symmetric key encryption, which means that all the cards and terminals store a secret data key that they use for authentication. If the card and terminal have the same secret key, they can send data back and forth. But if someone hacks one terminal or card and finds the key, then the entire system compromised. All of the cards and terminals have to be uploaded with a new key.

Inside Contactless has licensed public key encryption technology from NTRU, a startup in Burlington, Mass. Unlike other public key encryption systems, NTRU doesn't require a lot of processing power, uses very little storage on the chip and is fast, making it attractive for use in contactless smart cars. "We looked at RSA and other encryption technologies, but they were not as well suited to smart cards as NTRU's system," says Charrat.

Inside’s expects its next-generation contactless smart cards to be used for identification cards, transportation systems, electronic wallets and access control system. “The contactless smart card market is growing very vast,” says Charrat. “We are developing expertise that none of our competitors have.”