

## ELECTRONIC STAMPS LICK INTERNET SECURITY

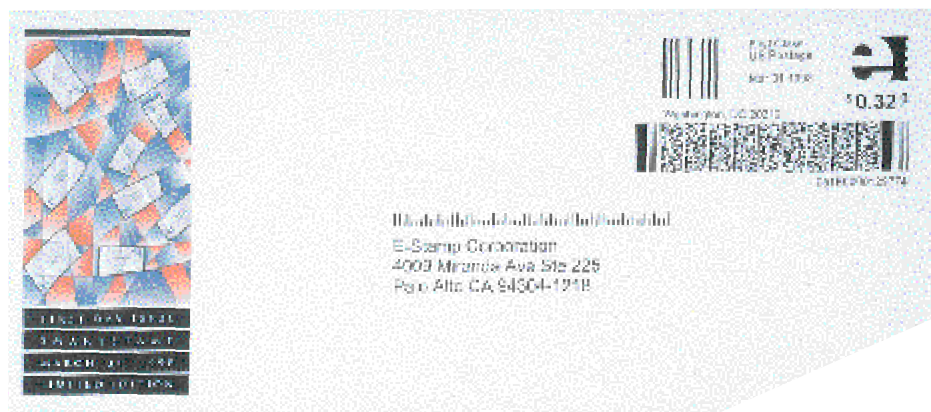
Thanks to cryptographic communications and a tiny electronic vault, you will soon purchase smart electronic postage stamps over the Internet and print them onto your envelopes with a conventional printer.

**WARREN WEBB, TECHNICAL EDITOR**

The idea of printing postage stamps onto the envelope when printing the address has been around for years, but there were plenty of problems. The US Postal Service wants to be sure that you have paid for the stamp that you are about to print, and they want to be able to detect multiple copies of the same stamp. Moreover, even if you are an honest user, what prevents a hacker

from stealing your authorization codes or stamp credits? The Postal Service initiated the Information-Based Indicia Program to search for solutions to these problems and to reduce the millions of dollars lost annually to fraud. (Indicia are postal markings on an envelope that replace a stamp.)

On March 31 of this year, the Postal Service approved beta testing of the



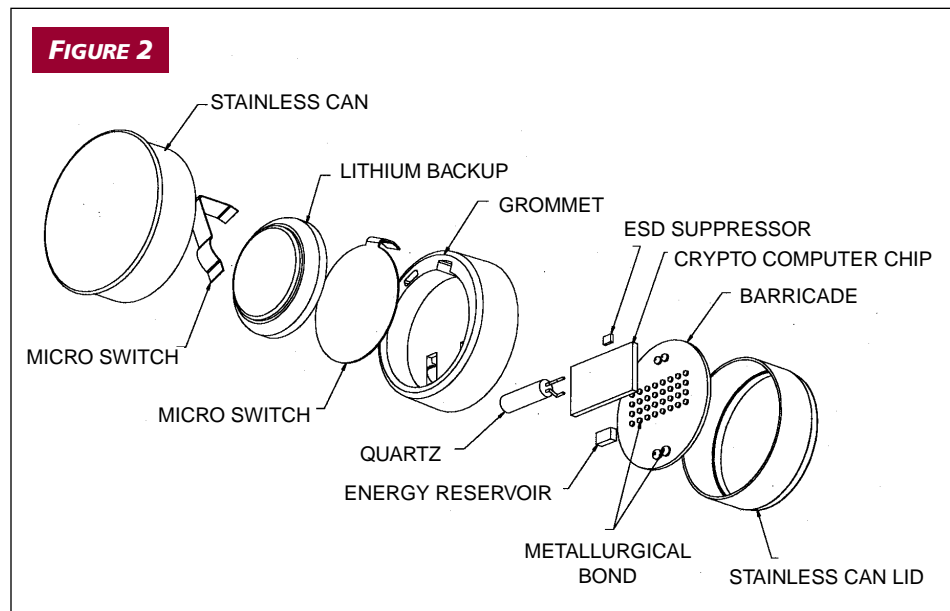
**FIGURE 1** A new electronic stamp with a 2-D bar code contains the postage amount, the source and destination zip codes, and the exact date and time the stamp was printed. Electronic stamps have the potential to provide tracking and tracing for individual letters.

## How it works

first Internet electronic-stamp delivery system, developed by E-Stamp Corp ([www.estamp.com](http://www.estamp.com)). Beta-test users can access an Internet-post-office Web site, sponsored by E-Stamp, to purchase and download electronic stamps. Users download stamps to an electronic postal-security device attached to the parallel port, which protects and keeps track of remaining postage. E-Stamp provides Windows-based software to interact with the postal-security device and to print the stamps. The system will cost users less than \$300/year plus postage.

An electronic stamp is a 2-D, machine-readable bar code that users can print by laser, ink-jet, or thermal printers (Figure 1). Each stamp contains a unique digital signature that the Postal Service can use to detect fraud and multiple copies. In addition to security information, the bar code contains the postage amount, the source and destination zip codes, and the precise time and date that the electronic stamp was printed. Users may also encode special service requests, such as address changes, into the stamp. To preserve privacy, the stamp does not identify the individual or company sending the letter. The Postal Service also plans to use the data from electronic stamps to document the mail type and delivery distance for future price-hike requests.

The postal-security device used with the E-Stamp system is a button-sized electronic vault from Dallas Semiconductor ([www.dalsemi.com](http://www.dalsemi.com)) called the Crypto iButton (Figure 2). The DS1954 contains an 8051-com-



**Encased in a steel shell, Dallas Semiconductor's Crypto iButton provides secure private-key storage, a high-speed math accelerator for 1024-bit public-key cryptography, and secure-message hashing.**

patible mP, a real-time clock, 32 kbytes of ROM, 6 kbytes of nonvolatile RAM, and an exponentiation accelerator for integers as long as 1024 bytes. The manufacturer packages the electronics in a heavy-duty, stainless-steel housing with tamper-detection circuitry that immediately erases critical data in the event of an intrusion. A metal-layer shield even detects attempts to microprobe the chip.

Designers optimized the Crypto iButton, which costs less than \$15, for public-key cryptography. Public-key cryptosystems rely on trap-door mathematical functions that are easy to perform in the forward direction but could take months or years to compute in the inverse direction. A private key, which the user keeps secret, gives information about the trap door and allows the software to easily compute the function in both directions. The E-Stamp system uses public-key cryp-

tography for both data encryption and digital signatures to protect the customer's account information during Internet-purchase transactions.

With a full-fledged cryptosystem to guard against hackers, the Postal Service is convinced that electronic stamps will replace the many postage meters designed for the home-office and small-business market. The Postal Service may have a point, because Microsoft ([www.microsoft.com](http://www.microsoft.com)) has purchased a 10% equity stake in E-Stamp. Microsoft would like to integrate electronic stamps directly into Word so users could both address envelopes and print stamps with a click of the mouse.

Although the technology is interesting, the average user is still interested in just getting his letter from point A to point B. So, after he prints this snazzy electronic stamp onto his letter and drops it into the nearest blue letterbox, will it get to its destination any faster? We will have to wait and see. Maybe it is still the same-old snail mail. EDN

You can reach Technical Editor Warren Webb at 1-619-513-3713, fax 1-619-486-3646, [wwwwebb@cts.com](mailto:wwwwebb@cts.com).

*The Postal Service is convinced that electronic stamps will replace the many postage meters designed for the home-office and small-business market.*