

GEMALTO TOKEN FOR WEB AUTHENTICATION/SECURITY

Most tokens designed to secure financial transactions on the Internet work either by making passwords more secure or by authenticating credentials between a customer and a Web site. Gemalto's new token does both, and does not require customers to download any



software in order for it to work. Called the Network Identity Manager (NIM), it is essentially a hardware-enclosed smart card, but

one that uses standard TLS/SSL Internet security rather than conventional smart card technology so it can verify Web sites by exchanging digital credentials. Instead of generating a one-time password to secure the delivery of login data, it delivers the customer's own user name and password automatically after establishing a secure connection. This protects login

data from capture by malicious software secreted onto a PC. The NIM was introduced in February and is being evaluated by several financial and online service providers in the U.S.

Companies issuing the NIM can decide to increase the number of sites it can log onto by enabling

it to work with Verisign's VIP (Verisign Identity Protection)

network — a group of businesses including Northern Trust, Charles Schwab, PayPal, eBay, and Yahoo that have agreed to share a common authentication standard. NIM issuers can also choose to sign their own partners, such as an Amazon.com-type e-commerce portal. Amol Deshmukh is Worldwide Marketing Manager for Network Identity Solutions at Gemalto in Austin, Texas, (512) 736-0151, amol.deshmukh@gemalto.com.



How the NIM Works

Registration: (1) the financial institution or other provider loads credentials onto the NIM and ships it to their customer, (2) the customer plugs the token into the USB port on their PC, (3) the NIM presents a window where the customer selects a PIN that will authorize the NIM from then on.

On subsequent visits: (1) the customer plugs the NIM into their PC, (2) an onscreen keyboard is displayed where the customer can enter their PIN using a mouse rather than keystrokes, which can be captured by malware, (3) the customer selects a site from a list of participating service providers, (4) the NIM launches the PC's browser and takes the customer to the selected site where credentials are exchanged and login data is delivered.

Posted with permission from The Nilson Report, Carpinteria, California, www.nilsonreport.com