



Network Identity Manager

Strong Mutual Authentication for Internet Users

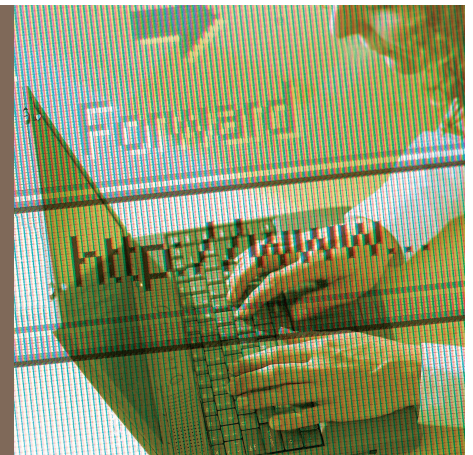
FINANCIAL SERVICES & RETAIL

ENTERPRISE

INTERNET CONTENT PROVIDERS > SOLUTION

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATIONS



Strong Mutual Authentication to Online Businesses, Fast and Simple

> Trust Is Essential for Internet Users

Portals, e-merchants and other trust-based network businesses depend on highly assured end-user identities for their success and survival. However, according to a 2005 survey conducted by the Cyber Security Industry Alliance, "...the fear of identity theft is keeping many consumers from doing business online, with 48% saying they avoid making purchases on the Internet because they are afraid their financial information may be stolen."

Unless consumers are absolutely confident that they are connected to a trusted site and their identity is secure, they will not conduct transactions online. In addition, they need to protect their online identity credentials for multiple web sites efficiently and conveniently. Conversely, online businesses and communities are required to maintain a minimal amount of personal information and they must keep it secure. Gemalto's Network Identity Manager solution makes it simpler and more secure for end users to conduct online transactions and participate in online communities and reduces the need for online businesses to store personal information.

> Connect with Assurance

Network Identity Manager is a smart card, browser-based strong authentication system that connects via a USB security device. It eliminates the need for additional server hardware, middleware and any client software on the user's PC. The user communicates with the smart card USB device through a Web browser and is authenticated to the device by entering a PIN.



Then, Network Identity Manager mutually authenticates the user and server through an encrypted end-to-end connection using standard security protocols. This makes the solution easier to implement and more secure than traditional multi-factor and mutual authentication systems.

Users can securely login to a remote server knowing their personal information remains private and that they are protected against password snooping, keyboard logging, spoofing, phishing, pharming, man-in-the-middle and Trojan attacks. Network Identity Manager provides an advanced level of security against these attacks by validating the relying party's public key and URL to values stored on the user's device through an encrypted end-to-end connection. In addition to

the smart card device, the essential task of managing the device is handled by a robust token management system that enables end-users to aggregate ID credentials for multiple trusted Web sites, manage their identities, and perform routine maintenance tasks such as updating information from trusted sites, unblocking PINs, and modifying security questions used for card unblocking.

> Network Identity Manager benefits

- Requires no client software for end-users
- Works with standard account privileges and browser settings
- Protects against password snooping, man-in-the-middle, keyboard logging, spoofing, phishing, pharming and Trojan attacks
- Standard USB form factor that is easily provisioned and deployed in high volumes
- Easily adapted to existing authentication architectures
- Use of Transport Layer Security (TLS) 1.0 protocol helps ensure hardware interoperability and component optimization.
- Support for Verisign VIP Network identity federation framework
- Multiple transaction partners can use the same end-user device, lowering operational costs
- Multiple language support facilitates worldwide deployment

Network Identity Manager Architecture

