In my continuing series of articles on identification and authentication (I&A), today I’d like to point readers to an interesting multi-factor authentication system that might be useful to you. After _Network World_ published an earlier paper in this series, I was contacted by a public relations officer for Privaris, Inc., a company founded in 2001 that concentrates on portable fingerprint-biometric I&A devices. The company description <http://www.privaris.com/company/index.html> explains that “Privaris has designed and developed a family of key-fob sized, personal, mobile devices that authenticate an individual's identity before interacting with their existing security systems used for granting access to buildings, offices, and garages (physical security), and computers, networks, and websites (logical security). Privaris products are targeted for use by the average consumer, small businesses, corporate enterprises of all sizes, and federal, state and local governments.”

Readers are aware that token-based authentication (“What you have”) suffers from a fundamental problem: the token can be used by anyone who finds or steals it if they know where it is to be used – just like an ordinary physical key can incorrectly allow a thief to open a car door lock. Privaris’ contribution is to allow the token to identify and authenticate its user using on-board biometric sensor and secure processor. Unauthorized personnel cannot use the tokens to impersonate the legitimate users: only the authorized, authenticated user can activate the device. The plusID™ “universal personal biometric device” has sufficient on-board processing power and storage to allow entirely local fingerprint recognition for authentication of identity. There is no backend database as is typically required with biometric solutions. The plusID™ can then interact with a wide range of existing systems by delivering standard credentials. For example, it has the ability to emulate a wide range of RFID access cards and can deliver cryptographic certificates for use in application-level identification and authentication.

The company offers a number of useful documents <http://www.privaris.com/resources/index.html> about plusID™ including a short white paper on “Achieving Universal Secure Identity Verification with Convenience and Personal Privacy” <http://www.privaris.com/pdf/Privaris_whitepaper_Universal%20Secure%20Identity.pdf> which has the following sections:

- Introduction
- Identity verification and multi-factor authentication
- Market adoption
- Making biometrics simple, secure and private
- Applications
- Compatibility with existing security infrastructure
- Using the device.

The paper states, “The plusID uses multiple wireless interfaces and USB to communicate with proximity and smart card readers, PCs, networks, and other security infrastructure. Different
plusID™ models offer various combinations of:

- 125 kHz RFID (proximity cards)
- 13.56 MHz RF (contactless smart cards - supporting ISO 14443 A and B, ISO 15693, and NFC)
- ISO 7816 & CCID compliant – compatible with standard Microsoft® Windows smart card infrastructure for computer logon
- Bluetooth™
- IEEE 802.15.4 (for long range applications such as gate access)
- One-time password capability (displayed via LCD and delivered wirelessly or over USB).

There’s an interesting recorded interview available from Network World Panorama with Privaris CEO John Petze available online <http://www.networkworld.com/podcasts/panorama/2007/091007pan-privaris.html> in which he discusses plusID™ with Jason Meserve. I enjoyed hearing Mr. Petze’s thoughts on the issues of I&A in a real-world environment where there’s an existing investment in authentication technology.

I think the technology looks promising, and, as Mr. Petze says in his interview, the price (currently in the $100/unit range) will undoubtedly go down as the underlying technology becomes less expensive and as sales volume increases.

[DISCLAIMER: As usual, I have no financial relationship whatever with Privaris, Inc.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.