Who are you? Mobile ID devices find out using NIST guidelines

August 26 2009

Mobile ID devices allow users in the field to collect biometrics and compare them with identity databases wirelessly. Credit: Orandi, NIST

A new publication that recommends best practices for the next generation of portable biometric acquisition devices -- Mobile ID -- has been published by the National Institute of Standards and Technology.

Devices that gather, process and transmit an individual's biometric data—fingerprints, facial and iris images—for identification are proliferating. Previous work on standards for these biometric devices has focused primarily on getting different stationary and desktop systems with hardwired processing pathways to work together in an interoperable

manner. But a new generation of small, portable and versatile biometric devices are raising new issues for interoperability.

“The proliferation of smaller devices including advanced personal digital assistants (PDAs), ultra-portable personal computers and high-speed cellular networks has made portable biometric systems a reality,” computer scientist Shahram Orandi says. “While the portable systems have made leaps and bounds in terms of capability, there are still intrinsic limitations that must be factored into the big picture to ensure interoperability with the larger, more established environments such as desktop or large server-based systems.”

The new mobile biometric devices allow first responders, police, the military and criminal justice organizations to collect biometric data with a handheld device on a street corner or in a remote area and then wirelessly send it to be compared to other samples on watch lists and databases in near real-time. Identities can be determined quickly without having to take a subject to a central facility to collect his or her biometrics, which is not always possible.

Soldiers are beginning to use these devices to control access to secured areas, and first responders can use them to ensure that only approved workers are on-site during an incident or investigation.

Special Publication 500-280: Mobile ID Device Best Practice Recommendation Version 1 offers guidelines to help ensure that, if followed, mobile and stationary systems will work together. It was developed by NIST researchers working with first responders, criminal justice agencies, the military, industry and academia.

For example, most current law enforcement applications require capturing all 10 fingerprints from an individual. Desktop fingerprint scanners provide a large scanning area—a platen—that can capture all 10

fingers in a fast, three-step process. Most portable devices, however, have platens that are a fraction of the size of a desktop scanner. The Mobile ID best practices publication provides guidelines that allow for the capture of all 10 fingerprints on a scanner with a smaller platen using a two-fingers-at-a-time approach.

The publication is available at fingerprint.nist.gov/mobileid/ … RS-20090825-V100.pdf .

Source: National Institute of Standards and Technology (news : web)