Biometric Web Services:
Interoperability for Multimodal Biometric Sensors

Ross J. Micheals
Supervisory Computer Scientist
National Institute of Standards and Technology
ross.micheals@nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Project Overview

- Design, develop, and implement a standard interface for interoperability of multimodal biometric sensors across heterogeneous IT environments.
- **Universal control of any biometric device, from anywhere**
- Previous work (including MBARK) focused on interoperability *within* a particular platform. The need for platform-specific *device drivers* leads to tight coupling between interface and *runtime*. (E.g., BioAPI & C, MBARK & .NET, Java BioAPI & Java)
- The World Wide Web can provide a rich interoperability platform

Web Services

- Same underlying protocol (HTTP), but instead of HTML (web pages), transfer XML (data)
- While HTML is meant for human consumption, XML is intended for machine (or application) consumption
- Simply consuming or generating XML does not guarantee interoperability. Standards are still necessary.

Impact of Web Services Interoperability

- **Physical Connectivity**
  - Before: USB or IEEE 1394 connection & device drivers
  - After: Ethernet or WiFi, no device drivers
- **Logical Connectivity**
  - Before: Logical attachment to specific machine. No device sharing.
  - After: Dynamic sharing from any Internet enabled device (different platforms, form-factors)

Technical Approach

- Conformance to the standard should imply a known-level of interoperability
- Support **remote multifactor authentication** and **mobile identification** applications
- Tiered levels of functionality
  - Level 1: Basic acquisition
  - Level 2: Live streaming
  - Level 3: Discovery, built-in asynchronous support
  - Level 4: Workflow?

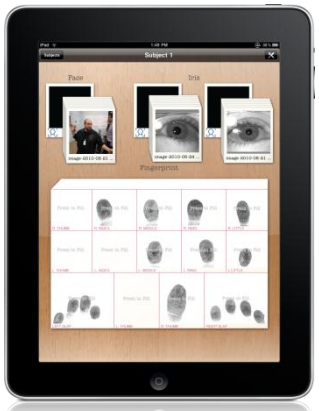
Technical Approach

- **Common approaches to Web services**
  1. *Simple Object Access Protocol (SOAP).*
     Formal OASIS standard with remote procedure call (RPC) like functionality
  2. *Representational State Transfer (REST).*
     General *architecture/guidance* of using XML/JSON over existing protocols.
- Many "low-powered" devices do not have comprehensive SOAP processing libraries. WS-Biometric Devices Level 1 is REST based to facilitate use on lightweight devices (phones, tablets, etc.)

Issues & Challenges

- Web services are inherently multiuser, but a biometric sensor is not. *Built-in concurrent access is required.*
- **Live preview may be challenging**
  - **Usability**: How do technological constraints effect end users? (operators, presenters, examiners)
  - What is the optimal format (Sequence of images? H.264?)
- **Multilayered security**
  - Currently only one popular sensor on the market encrypts sensor to computer communications
  - Data link layer: WPA2
  - Transport layer: SSL (HTTPS). Client-side certificates might be used for point-to-point authentication
  - Should payloads be encrypted? (ACBio?)

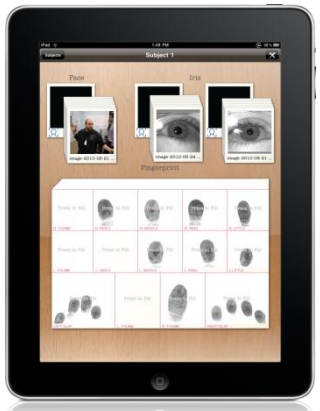
Demonstration System



Demonstration System

Sensor attached to small form-factor PC with WiFi

WS-Biometric Devices "server" adapts device driver to web services



Custom application on tablet that otherwise has no biometrics support

Web service could be embedded in device itself

Announcement

New OASIS TC Discussion list

bws-discuss

for evaluating the feasibility of creating a new OASIS Technical Committee for

biometrics & web services

bws.nist.gov

NIST
National Institute of Standards and Technology
U.S. Department of Commerce