Biometrics in a Networked World

Kevin Mangold, NIST Computer Scientist

kevin.mangold@nist.gov

July 23, 2012

Biometrics is generally used within a closed system, for example, an acquisition station may have a single, tethered connection to a biometric sensor requiring the presence of proprietary software. This setup has advantages: (1) it can provide an entire system from a user interface to sensor drivers to the biometric sensor itself; and (2) the user interface may be tailored to the specific device and features that it offers. On the downside, however, interoperability is reduced. If you change the biometric sensor from one model to another, updated software and a new user interface would be required. That is definitely not desirable—having users become familiar with a completely new system costs time and money.

Two new specifications integrating web services into a biometrics system have recently been published: Specification for WS-Biometric Devices (WS-BD), developed by the NIST Biometric Web Services team and published as NIST Special Publication 500-288 [1], and Biometric Identity Assurance Services (BIAS) SOAP (Simple Object Access Protocol – a type of web service) Profile, developed by OASIS BIAS Integration TC.

Why two different standards related to biometrics?

Two very important aspects should be taken into consideration when defining each system component: the scope of the component (what the component performs) and how the component interacts with external components. If you think about a system as a collection of building blocks, the scope is the size of the block and the shape of the block defines how it may interact with other components.

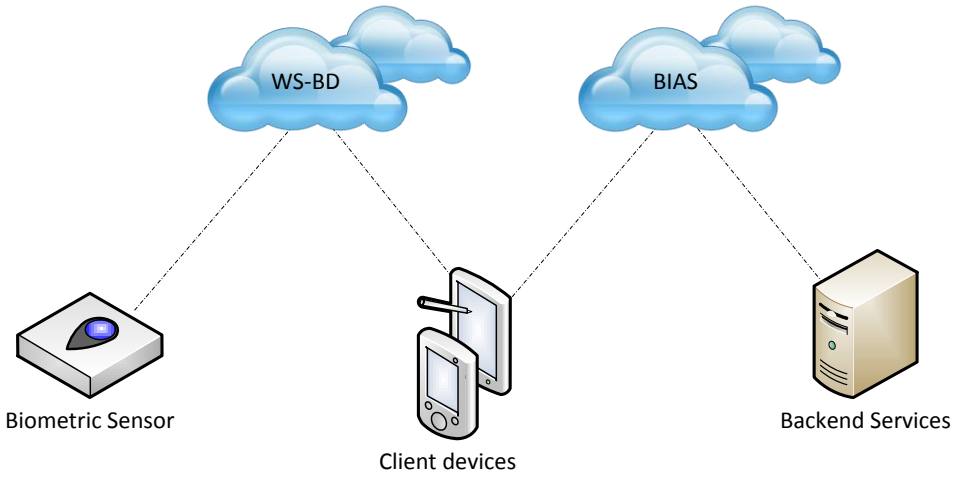
There are many advantages to using web services. First, it builds off a well-vetted protocol that has been used for decades, the Internet. By leveraging the Internet, we can take advantage of security features provided by HTTP/HTTPS (HyperText Transfer Protocol/Secure). Second, at their core, web services are just structured communication over the Internet; any device or operating system that is Internet-capable is able to use these specifications. And finally, web services provide an effective approach for developing and implementing distributed and service oriented applications and systems.

BIAS is a framework for developing, deploying, and invoking biometric identity operations over SOAP (Simple Object Access Protocol). BIAS describes operations at varying levels and can support primitive and/or aggregate operations. The aggregate operations include enrollment, identification, verification, and querying for service capabilities.

WS-Biometric Devices is a REST-based web service specification for the command and control of biometric acquisition devices. REST, which stands for Representational State Transfer, is an architectural style for designing and implementing web services. WS-BD provides an approach to developing a web-

based interface to and from biometric devices in a modality-agnostic manner. It contains support for common operations such as session registration, service locking (for exclusive access), capture, download, and metadata. A WS-BD client does not need to know what type of modality a particular sensor captures to allow for communication. This separation of communication methods and types of sensors allows a high degree of interoperability and the ability to swap out sensors with minimal modifications to the client.

BIAS and WS-BD are not competing specifications; instead, they complement each other. Imagine a system of multiple kiosks, each consisting of a fingerprint scanner and face scanner. Each kiosk is remotely monitored by someone using a tablet to control various actions. It is important to note that someone does not need to be physically present at each kiosk—using web services makes it easier for one person to monitor multiple kiosks. Once the biometric information is captured and received by the remote monitoring station, it can then be transmitted over a network to a biometric identity management service for enrollment, verification, or identification. Each component of this biometric system can be physically as close as inches or as far away as miles. Because everything is done over a secure network connection, control can be handled by any device that is Internet-capable (for example, smartphones, tablets, or laptops), in addition to the workstations and servers used in the past.

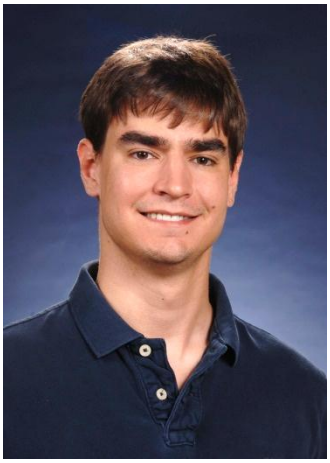


The rapid evolution of technology and the Internet has revolutionized the way we complete our work and communicate with each other. Specifications such as BIAS and WS-BD help push biometrics and biometric operations into the future by offering a free and open solution to substitute proprietary communication methods and software while, at the same time setting the stage and precedent for future biometrics and communication specifications.

References:

[1] National Institute of Standards and Technology Special Publication 500-288, *Specification for WS-Biometric Devices (WS-BD)*, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=910334, March 2012

About the Author



Kevin Mangold is a Computer Scientist at the National Institute of Standards and Technology (NIST). His work includes biometric standards development, identity management, and biometric technologies research with a high degree of focus on interoperability and web services. He is very active in ISO/IEC JTC 1 SC 37 subcommittee on biometrics, INCITS M1 technical committee on biometrics, and co-chairs the Biometric Identity Assurance Services (BIAS) Integration technical committee at OASIS.