Applying Technical Standards to Biometric Systems

Milorad Milinković, Faculty of Organizational Sciences, University of Belgrade, Belgrade, Serbia
Miroslav Minović, Faculty of Organizational Sciences, University of Belgrade, Belgrade, Serbia
Miloš Milovanović, Faculty of Organizational Sciences, University of Belgrade, Belgrade, Serbia

ABSTRACT

Nowadays, the development and the application of biometric systems on one hand, and the large number of hardware and software manufacturers on the other, caused two the most common problems of biometric systems: a problem of interoperability between system’s components as well as between different biometric systems and a problem of biometric data security and privacy protection, both in storage and exchange. Specifications and standards, such as BioAPI and CBEFF, registered and published as multiple standards by ISO (International Organization for Standardization), propose the establishment of single platform (BioAPI) to facilitate the functioning of the biometric systems regardless of hardware or software manufacturers, and unique format for data exchange (CBEFF) to secure biometric data. In this paper, these standards are analyzed in detail and considered as possible solutions to aforementioned problems.

KEYWORDS

INTRODUCTION

At the beginning, the term of interoperability should be defined. Li and Jain (2009, p. 27) state that “interoperability in the field of ICT includes the use of the same format or protocol without disrupting the performances of the system”. According to Wayman, Jain and Maltoni (2005) this is related to the functioning and communication between parts of the same system, as well as cooperation and communication between various systems.

Since Biometrics is increasingly presented on the market (for example, according to Ryan (2009) enterprise-wide network security infrastructures, employee IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefitting from biometric technologies), and as Li and Jain (2009, p. 18) point out that “Biometrics uses physical or behavioral characteristics of an individual to uniquely identify the user during authentication”, the security of information as well as communication between the parts of a biometric system must be at the highest level. Deravi (2008, p. 34) discusses that “due to the fact that the development of biometric technologies and devices, as well as software applications, gained the momentum, there was the problem of large number of manufacturers and the problem of communication between software and devices from different manufacturers (so-called “vendor lock-in”)”. Considering those facts, lack of unique platform as well as a unique format for information exchange between components of one biometric system, or between different biometric systems has become the big problem.

Barrera, Alcántara, Alegría, Ávila and Esparza (2009) discuss that compliance with international standards allows bridging the gaps between the different data sources and allows transparent access.
to the information of the dissimilar sources to enable their joint exploitation (in our case sources are: databases, system’s components, systems). So, as it stands in The BioAPI Consortium report (“BioAPI Specification Version 1.1”, 2001), in 1998 BioAPI Consortium has been formed with the main aim to create BioAPI specification and define a unique platform for communication between applications and biometric technologies regardless of the manufacturer. Subsequently, BioAPI with the status of an international standard should accelerate the acceptance of biometric technologies and a large number of commercial applications at the international level.

On the other hand, as Deravi (2008) points out, since there was no single format that would facilitate the exchange of biometric information, cooperation between NIST Institute and BioAPI Consortium has formed CBEFF (Common Biometric Exchange Formats Framework) as an idea to establish a unique format for the exchange of biometric information between different systems with an emphasis on data security. Primarily, the format for the exchange of fingerprints was established, followed by NISTIR 6529 specification, which applies to all biometric modalities, today now known as CBEFF. The current version NISTIR 6529-A is an extended version of CBEFF which, unlike previous versions, may contain information of various biometric modalities at the same time or more information of a single modality. According to Matyas and Stapleton (2009), this standard establishes appropriate security requirements that will allow different biometric solutions to co-exist in the marketplace. Also, this standard views biometric systems within a global user community and it assures that the security of any one biometric system will be unaffected by the security of any other biometric system.

Lockie (2002) highlights that BioAPI and CBEFF were originally designed to help integrate biometrics in client-server scenarios, in particular, to introduce biometric identification in the internet applications. The significance of BioAPI and following CBEFF is that more than 90 worldwide companies and organizations took a place in their designing. According to Sanchez-Reillo, Alonso-Moreno, Fernandez-Saavedra, and Kwon Y-B (2012) standardized biometric technology is able to provide for developers in biometrics and third parties with a way to perform comprehensive evaluations remotely and with 24/7 availability without compromising the privacy of the individuals included in the test crew.

In this paper, these specifications (adopted international standards as well) are described through examples in detail. We used literature review as a research methodology, gathered information via the internet from the credible sources such as reports from Standardization Bodies (ISO, NIST, BioAPI Consortium) and papers, chapters and books from prominent authors in the relevant scientific field. Then we applied analysis method to evaluate collected information and to decide whether BioAPI and CBEFF are suitable solutions for aforementioned problems of biometric systems.

BIOAPI SPECIFICATION

Jain, Flynn and Ross (2008, p. 399) highlight that “BioAPI is a standard that defines a simple biometric application interfaces, a standardized modular approach to biometric functions, algorithms, and devices, a standardized methods for distinguishing biometric data and device types, and a support for biometric identification in distributed computer environments”.

Lockie (2002) points out that BioAPI provides a high-level generic biometric authentication model, suited for any form of biometric technology. In the ISO/IEC 19784-1:2006 Standard (2015) an architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs), corresponding Service Provider Interfaces (SPIs), and associated data structures. In the ISO/
Effective and Efficient Classification of Topically-Enriched Domain-Specific Text Snippets: The TETSC Method
[www.igi-global.com/article/effective-and-efficient-classification-of-topically-enriched-domain-specific-text-snippets/136282?camid=4v1a](www.igi-global.com/article/effective-and-efficient-classification-of-topically-enriched-domain-specific-text-snippets/136282?camid=4v1a)

Strategic Approach towards Clinical Information Security
[www.igi-global.com/chapter/strategic-approach-towards-clinical-information-security/138652?camid=4v1a](www.igi-global.com/chapter/strategic-approach-towards-clinical-information-security/138652?camid=4v1a)

A Federative Approach of Decision-Making Aid in Urban Development
[www.igi-global.com/chapter/federative-approach-decision-making-aid/11275?camid=4v1a](www.igi-global.com/chapter/federative-approach-decision-making-aid/11275?camid=4v1a)