# Are Biometric Web Services a Reality?
## *A Best Practice Analysis for Telebiometric Deployment in Open Networks*

Dustin van der Haar and Basie von Solms
*Academy of Computer Science and Software Engineering, University of Johannesburg, Cnr Kingsway and University Road, Auckland Park, Johannesburg, South Africa*

Keywords: Telebiometrics, Policy, Services, Distributed Access Control.

Abstract: With the growth of biometric system complexity and the resources required for these systems, newer biometric systems are increasingly becoming more distributed to deal with accessibility and computation demand. These telebiometric systems introduce additional problems, which are outside of the scope of traditional biometric standards. Best practices have been published that address problems in these distributed systems, by outlining service-based approaches that provision typical biometric operations through the use of telecommunication standards, such as SOAP. In this paper, 2 families of best practices for telebiometric-based systems (the ITU-T X.1080 family of recommendations and the BIAS family of standards) are reviewed and assessed according to their current deployment potential within an online context. Recommendations are then presented and a verdict is given that shows current best practice provides adequate guidance for the building of large-scale telebiometric systems that utilise web-based biometric services.

## 1 INTRODUCTION

As a human being we take many things for granted such as walking, talking or breathing. In order to coordinate these various activities, a multitude of physical systems all work together to accomplish the goal at hand. Aside from enabling us to perform these and many other tasks, the physical parts or attributes for each human being are all unique. The measurements derived from these physical or behavioural attributes, which are used to achieve automated recognition, are called biological metrics or biometrics. It is these measurements that have helped us reach a form of identifying and authenticating human beings, which surpass conventional username-password and token paradigms, with regards to convenience and security.

In the past, the lack of robust measuring tools or sensors limited the use of certain biometrics to facial attributes, fingerprints, hand geometry and other established biometrics (Woodward et al., 2003), but as technology improves, so does the rise of new and ever improving biometrics used in society today, such as (Sarkar et al., 2010; Shen et al., 2012). One domain that has relatively less potential for using biometrics (when compared to physical environments) is open networks found in the public virtual domain or online spaces, where various service providers, such as social networks, online shopping and premium content providers reside. The problem with this domain is that many biometrics measure physical presence, and the virtual presence that exists in these open networks lacks certain attributes that can be measured with little effort and therein lies the root of the problem. Effective biometrics used in an online environment are limited to biometric attributes that are carried over to this virtual presence and in some cases, it is difficult to identify and deploy biometrics that are cost effective and compatible with modern public open networks.

In addition to identifying potential biometrics that can be used in this environment, it is a difficult task to choose the best biometric for a specific environment. Although guidelines and best practices exist to facilitate authentication and interoperability for telebiometric systems (ITU-T, 2008a), these best practices lack guidance for choosing good biometrics to deploy in virtual or online spaces. Further guidelines that address biometric choice in a domain should narrow the decision-making process and mitigate problems that could result in deployment failure, poor user acceptance and unnecessary costs.

The paper will begin with a brief background on telebiometrics, along with how biometrics are evaluated to determine which biometric should be chosen. Following that, a best practice analysis will be


van der Haar D. and von Solms B..
Are Biometric Web Services a Reality? - A Best Practice Analysis for Telebiometric Deployment in Open Networks.
DOI: 10.5220/0004521704940499
In *Proceedings of the 10th International Conference on Security and Cryptography* (SECRYPT-2013), pages 494-499
ISBN: 978-989-8565-73-0

performed that addresses the potential deployment of biometrics within a public open network context. Recommendations then follow, which should help address any issues identified and the paper is then concluded.

## 2 PROBLEM BACKGROUND

Human beings have been identifying people with physical or behavioural traits for many years ranging from hand or finger impressions on artwork, to even using an individual's DNA to solve crimes. The abundance of these unique characteristics that humans exhibit, leave almost endless possibilities for identification and provide a good means to determine if a person is exactly who they say they are (authentication). These biometrics have especially been useful to ensure the latter in many organisations to protect physical environments, which contain valuable company assets, from unwanted individuals that may want to steal or damage these assets. By applying biometrics to telecommunication and changing how biometric sensing works with telecommunications, telebiometrics are formed.

### 2.1 Telebiometrics: Biometrics as Online Authenticators

The protection of physical environments may be an established field, but the application of these techniques within an online context is lacking. Although the amount of open networks and virtual assets that need protection are growing, as seen in open network services, the variety of online mechanisms that protect these assets from unauthorised access are not. The majority of the mechanisms that limit access to these virtual environments, employ the username-password paradigm. Just as limitations of the username-password paradigm have been encountered in physical environments, so do many of these problems carry over into an online context. Passwords can be forgotten, stolen without the user's knowledge and can be derived should the password length be inadequate (O'Gorman, 2003). However, unlike tokens, which have a limited amount of potential within the online context, passwords can be easily used to protect access to open networks.

In a similar manner to token-based systems, biometric systems typically measure attributes with sensor equipment specialised for a specific biometric, such as a fingerprint scanner, making a transition from the physical environment to the online public domain difficult. The additional costs the equipment introduces to the end user, make it difficult to deploy and gain user acceptance, especially if users need to purchase the equipment themselves. However, not all sensors for biometric systems need to be purchased separately. There are certain sensors, such as cameras, microphones, keyboards and mice, which all have the potential to capture biometric attributes. By utilising these sensors that extend the reach of attributes to a user's virtual presence and keeping environmental constraints in mind, face recognition (Woodward and Corporation., 2003), speaker verification (Kelly et al., 2012), mouse dynamics (Shen et al., 2012) and other biometric mechanisms, can be used to authenticate users in open networks.

Although many other biometric systems can be deployed in a public open network by simply modifying the communication channel used between components into a web service-based channel, factors exist that differentiate it from the average physical deployment. If the communication channel is not protected properly, it can be attacked to compromise the system, because communication occurs within a public domain (Buhan and Hartel, 2005; ITU-T, 2008b). Managing the distributed system also becomes a more difficult task and the points of potential failure increases due to the additional mechanisms included to facilitate telecommunication. In a public domain, users are individuals that have subscribed for a service, such as social networking or online media viewership, and do not necessarily have certain biometric sensors at their disposal, such as fingerprint scanners. Should the biometric system require the user to purchase additional equipment in order to be identified or authenticated, unnecessary inconvenience is incurred that directly affects the uptake of the system and potentially the service.

### 2.2 Current Best Practice for Telebimoetrics

Currently, standards in force that show promise to address telebiometrics and their respective issues include, the International Telecommunication Union X.1080 family of standards, the OASIS BIAS, BIAS SOAP Profile and NIST 500-288 family of standards. These standards address conformance, configuration and to a larger extent, interoperability within a telecommunications context. In the following segments, a brief overview of these standards are provided as a precursor to the best practice analysis in the next section.

#### 2.2.1 ITU-T X.1080 family of Recommendations

One of the existing best practices provided for telebiometrics, ITU-T X.1081 (ITU-T, 2011) and X.1084 (ITU-T, 2008a), addresses user interactions, measurements, authentication and system configuration in open network systems, by providing biometric authentication protocols and profiles for telecommunication systems. It dictates how unspecified end users and service providers should communicate during authentication, along with the roles the associated servers and clients play when facilitating authentication. Nine authentication models and profiles are introduced to accommodate different locations of the biometric database and comparison components. The authentication models namely, Local, Download, Attached, Centre, Reference Management on TTP for local, Reference Management on TTP for centre, Comparison outsourcing by client, Comparison outsourcing server, Storage and comparison outsourcing by client and server, are derived from existing policies. By drawing on existing standards in telecommunications (such as ITU-T X.509), the biometrics domain (X9.84-CMS) and BioAPI (ANSI/INCITS, 2002) to interface with sensors and facilitate communications, a secure platform is formed that is reliable and interoperable with current systems. Although related recommendations deal with important aspects such as authentication infrastructure (ITU-T, 2008c) and security countermeasures (ITU-T, 2008b), as we will see in the review, the current ITU-T X.1080 family of recommendations lack certain guidelines necessary for effective telebiometric system deployments.

#### 2.2.2 BIAS and NIST 500-288 Family of Standards

Another newer set of standards that specifically target provisions required for telebiometrics is the ANSI INCITS 442 BIAS standard (ANSI/INCITS, 2010) and the OASIS BIAS SOAP Profile (OASIS, 2012). The BIAS standard defines how identity assurance can be provided with biometric services that work over a service oriented architecture (SOA). It differentiates between biometric operations and data elements, along with its associated requirements, such as how to manage biometric data, along with bridging the gap between business operations and a distributed biometric system. The standard also specifies modular operations and the inclusion of the CBEFF standard (ISO/IEC 19785 1:2006) for data representation, as well as the established BioAPI standards ((ANSI/INCITS, 2002) and ISO/IEC 19784-1) for added flexible interfacing and draws on existing biometric expertise. The OASIS BIAS profile aims to provide conformance with backend biometric services (specified by BIAS) and adequate binding to target web environments, by outlining biometric methods that use SOA messaging formatted by the XML defined in the BIAS standard (the data elements). The profile also provides a comprehensive set of guidelines that addresses aggregate operations such as enroll, identify, verify and retrieve information, which are required for tasks in a biometric system. Collectively these standards provide an open framework that can be used in public open networks.

The standard that accompanies the BIAS and the BIAS SOAP Profile, the National Institute of Standards and Technology (NIST) 500-288: Specification for Web Services for Biometric Devices (WS-BD) (Micheals et al., 2012) provides a command and control protocol for biometric devices in open networks, thereby extending the acquisition process. By focusing on an acquisition process that is device, operating system and channel independent, interoperability is achieved with any component that is REST (Representational State Transfer) compatible. The components include a client, sensor and sensor service, which facilitate acquisition requests, capture biometric samples and provides middleware, respectively, for the acquisition process. Service behaviour, message formats, configuration and operations are outlined with the aid of existing standards published by the IETF, ISO and NIST itself. Operations such as registration, locking, information, initialisation, configuration, capture, download and cancellation all help to facilitate the extended acquisition process, required for this level of interoperability. The standard also already has Java and .NET implementations (which can be found at (NIST, 2013)) that make deployment easier. The combination of BIAS, the BIAS SOAP Profile and the WS-BD specification collectively provide a good platform to provide web service-based telebiometric systems, which is readily available to service providers. Although these standards address some of the issues the ITU-T X.1080 family experiences, they too lack certain guidelines necessary for public open network deployment.

#### 2.2.3 Best Practice Alternatives

The above best practice directly addresses telebiometric systems, or extend regular biometric systems to telebiometrics systems. However, other technical interface, data interchange, profile, testing and reporting standards can be modified or replaced to form more customised guidelines, such as (Otero-Muras et al., 2007). These customised guidelines should work well in organisations that already have biometric guidelines in place, such as the US government,

Interpol and other law enforcement agencies. Adopting this approach though, will lower expected interoperability and conformance when integrating these systems with other agencies.

# 3 BEST PRACTICE ANALYSIS

For years there was a gap in best practice on biometric services and their application in open networks. From the mid-2000s standards organisations have been trying to address this gap and currently are moving towards full implementations, making biometric services a reality to distributed agencies that are in dire need of telebiometric systems. In this section, each of the previously identified telebiometric-based best practice families are reviewed according to their current deployment potential.

## 3.1 ITU-T X.1080 Family

The first family of best practice provides comprehensive material on telebiometrics, by specifically outlining (in (ITU-T, 2011)) the type of basic interactions or modalities that biometrics are derived from and expected units of measure. By utilising the BioAPI framework and coordinating it with X.1083 (ITU-T, 2007) and X.1084 (ITU-T, 2008a) a bridge is successfully formed between the biometric and the telecommunications domains. However, there is a lack of conformance that still needs to be addressed for it to fully comply with the BioAPI specification. Another issue that may be a problem for open networks is that only a local registration or enrolment has been outlined in X.1084. The lack of a remote registration will cause inconvenience among users in public open networks. Although this constraint is mainly there to prevent fraudulent registration, more research should be done to introduce a trusted registration process that strikes a balance between security and convenience. Another problem related to the registration process is that there is a lack of explicit guidelines when dealing with biometric revocation. There needs to be finer guidelines that deal with partial revocation and full revocation, instead of just specifying a template update process.

## 3.2 BIAS and NIST 500-288 Family

The next family of best practices outlined, also leverages a great deal of its specification on existing standards, which eliminate teething issues that sometimes occur with new best practices. Its modular structure makes it flexible when addressing business processes and makes it compatible with many existing platforms. It even includes operations that are missing from the ITU-T X.1080 family of recommendations, such as a quality check, a conformance check and enrolment that can potentially be used for remote registration. However, it too suffers from a limited amount of guidelines when dealing with biometric revocation. One minor problem that the BIAS family of standards exclusively experiences is a lack of service guarantees, quality assurance or a way to measure service workload so that the binding layer (in this case the BIAS SOAP Profile) is appropriately informed.

## 3.3 Overall Analysis

Both best practice families outline the basic requirements and core elements required for telebiometrics, such as how information should be presented and exchanged between entities. They both use the well-established BioAPI framework, which already aids in further interoperability. However, it is unclear how these mechanisms will perform in very large scale applications. The authors have discovered (based on (Jain and Kumar, 2010)) that it is difficult to address large-scale application deployments, because biometrics utilised on this scale must be able to deal with the following requirements:

1. The system must maintain a high accuracy and throughput under varying operating conditions and user composition.
2. The deployment must maintain high sensor interoperability.
3. The system needs to be able to perform rapid collection of biometric samples, even during harsh operating environments.
4. The system must provide high levels of privacy and template protection.
5. There must be secure support structures in place for operations.

In typical biometric systems a compromise is usually met that fulfills these requirements according to the amount of resources available. Although certain aspects such as sensor interoperability, privacy and template protection, are already addressed by current best practice, it will be a difficult task to address these requirements on a large-scale in public open networks.

Another consideration that warrants attention is the deployment of biometrics to public open networks and the constraints it introduces to the environment. The larger realm of the Internet introduces many variables that may or may not affect the potential telebiometric system and identifying these variables and de-

termining their resultant effect on the system is a task that also needs to be addressed.

Although the BIAS standard briefly mentions service level monitoring, in both standards there is a lack of mechanisms for non-repudiation and an appropriate audit trail that can be used to mitigate service abuse and potential subversion attempts. The distributed nature of telebiometric systems, makes non-repudiation necessary, because of the increased risk introduced by extending the communication channel to an open network.

# 4 PROPOSED RECOMMENDATIONS

In this section, possible recommendations identified by the authors are outlined that may improve current specifications in the highlighted areas.

## 4.1 Evaluating Biometrics for Deployment

Many of the problems related to deployment can be mitigated if a more detailed investigation is pursued while the deployment of the respective telebiometric system is considered. The problem, however, is that many organisations do not have access to the resources, such as skilled individuals or information, to make better decisions on which biometric to deploy and how the deployment should be done. The problem does not just stop there. Even with the resources, every environment is unique and it may exhibit a new set of constraints that other environments may not experience. Best practices can be integrated that outline this investigative process in order to help with determining the best biometric fit for a specific environment. By identifying environmental requirements and constraints, along with a biometric with the appropriate level of usability, as guided by (NIST, 2008), a better biometric system with fewer errors will be implemented and deployment should be easier.

## 4.2 Open Enrolment

Another topic brought up in the review is that some standards (namely the ITU-T X.1080 Family) only have provisions for local or face-to-face enrolment, thereby causing user inconvenience. This approach may still have merit when users are within a reasonable distance from an enrolment centre, because these centres are trusted and will have less fraudulent enrolments. However, when these centres become unreasonably far from users and the biometric sensors are readily available to them, a compromise may need to be made to accommodate them. One approach is to introduce a remote enrolment centre that establishes trust between the user and the center, in a similar manner to the approaches found in (Jsang et al., 2007). After trust has been established, enrolment can commence and when the acquisition process is followed, a quality check can be performed on the received biometric sample to gain a viable sample and to reduce subsequent errors in authentication. Depending on the level of security required, the provisioning of this process can be changed from completely omitting open enrolment for high security environments, to providing open enrolment with limited authority rights.

## 4.3 Biometric Revocation

One area in the field of biometrics that receives a great deal of criticism is the revocation of biometrics. If a user's biometric has been compromised, the system should revoke the biometric and every time that biometric is presented, authentication should fail. However, if this biometric is used in other systems, revocation presents a real problem. One approach is to use multiple biometrics and upon revocation, the alternative biometric can be used. However, a more viable approach is to use a cancelable biometric template (Teoh et al., 2006) and should biometric revocation occur, another template can be generated, using the same biometric. Best practice can be introduced that outlines this process, as well as its requirements.

## 4.4 Non-repudiation and Regulation

Another topic addressed in the review is the monitoring and recording of user activities that occur in a system. By including a lightweight non-repudiation protocol (Zhou and Gollman, 1996) within biometric services, which can be reviewed by a trusted third party or a quality assurance component, liability can be successfully tied to component activity. This is especially needed in distributed systems where activity can be contested and abuse occurs. Should any component facilitate biometric operations, that component will be accountable for the resources used for that operation. Services can be regulated based on the recordings, to provide a fair service to other components that require the service. Best practice can also be included to deal with requirements for non-repudiation and regulation, as well as outlining the role of the trusted third party.

## 5 CONCLUSIONS

Overall, current best practices in both families have shown that biometric web services are a reality and future implementations should benefit greatly from them. Current developments, such as the implemented fingerprint-based telebiometric system using the WS-BD specification, updates to the BioAPI framework and further standardisation of BIAS into ISO/IEC 30108, further support this claim. However, there are still adjustments that need to be made by the ITU-T Study Group 17, INCITS M1 Technical Committee and other policy makers to reach large-scale telebiometric systems of tomorrow.

## REFERENCES


ANSI/INCITS (2002). Ansi/incits 358 - the bioapi specification. Technical report, American National Standard for Information Technology.

ANSI/INCITS (2010). Information technology - biometric identity assurance services (bias). ANSI INCITS 442-2010.

Buhan, I. and Hartel, P. (2005). The state of the art in abuse of biometrics.

ITU-T (2007). Itu-t recommendation x.1083 : Information technology - biometrics - bioapi internetworking protocol. Technical report, International Telecommunication Union.

ITU-T (2008a). Itu-t recommendation x.1084 : Telebiometrics system mechanism part 1: General biometric authentication protocol and system model profiles for telecommunications systems. Technical report, International Telecommunication Union.

ITU-T (2008b). Itu-t recommendation x.1086 : Telebiometrics protection procedures - part 1: A guideline to technical and managerial countermeasures for biometric data security. Technical report, International Telecommunication Union.

ITU-T (2008c). Itu-t recommendation x.1089 : Telebiometrics authentication infrastructure (tai). Technical report, International Telecommunication Union.

ITU-T (2011). Itu-t recommendation x.1081 : The telebiometric multimodal model - a framework for the specification of security and safety aspects of telebiometrics. Technical report, International Telecommunication Union.

Jain, A. and Kumar, A. (2010). *Biometrics of Next Generation: An Overview*. Springer.

Jsang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618 – 644. Emerging Issues in Collaborative Commerce.

Kelly, F., Drygajlo, A., and Harte, N. (2012). Speaker verification with long-term ageing data. In *Biometrics (ICB), 2012 5th IAPR International Conference on*, pages 478 –483.

Micheals, R. J., Mangold, K. C., Aronoff, M. L., Kwong, K., and Marshall, K. (2012). Specification for ws-biometric devices (ws-bd). NIST SP - 500-288. http://bws.nist.gov (Last Accessed 16/12/2012).

NIST (2008). Usability & biometrics - ensuring successful biometric systems. Technical report, National Institute of Standards and Technology. http://zing.ncsl.nist.gov/biousa/ (Last Accessed 19/12/2012).

NIST (2013). Nist 500-288: Biometric web services. National Insitute of Standards and Technology (NIST).

OASIS (2012). Biometric identity assurance services (bias) soap profile version 1.0. OASIS Standard. http://docs.oasis-open.org/bias/soap-profile/v1.0/os/biasprofile-v1.0-os.html (Last Accessed 18/12/2012).

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021 – 2040.

Otero-Muras, E., González-Agulla, E., Alba-Castro, J., García-Mateo, C., and MÁrquez-Flórez, O. (2007). An open framework for distributed biometric authentication in a web environment. *Annales Des Télécommunications*, 62:177–192.

Sarkar, I., Alisherov, F., hoon Kim, T., and Bhattacharyya, D. (2010). Palm vein authentication system: A review. *International Journal of Control and Automation*, 3(1):27–34.

Shen, C., Cai, Z., Guan, X., and Wang, J. (2012). On the effectiveness and applicability of mouse dynamics biometric for static authentication: A benchmark study. In *Biometrics (ICB), 2012 5th IAPR International Conference on*, pages 378 –383.

Teoh, A., Goh, A., and Ngo, D. (2006). Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 28(12):1892 –1901.

Woodward, J. and Corporation., R. (2003). *Biometrics : A Look at Facial Recognition*. RAND, Santa Monica, Calif.

Woodward, J., Orlans, N., and Higgins, P. (2003). *Biometrics*. Rsa Press Series. McGraw-Hill/Osborne.

Zhou, J. and Gollman, D. (1996). A fair non-repudiation protocol. In *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, pages 55 –61.