Title: Web Services-Based Operational Monitoring and Reporting
Proposer: Optimum Biometric Labs AB
Proposed Lead Editor: Babak Goudarzipour

Dear Kevin, Dear OASIS board and members,

We would like to propose a New Work Item to initiate an OASIS standard in Web Services-Based Operational Monitoring and Reporting. This is associated with biometric-based verification and identification systems and applications.

Introduction

In the era of Internet-of-Things, Cloud Computing, and Big Data it becomes an increasingly vital capability for operators and system owners to

- instantly and remotely know what is going on with their resources,
- to improve overall system quality and usability or assist individual users with usage difficulties,
- to prevent issues and proactively pinpoint and resolve early warnings and problems,
- and to optimize site maintenance and management while minimizing the associated costs

This is a well-established area in diverse industries (such as Aerospace and Rotating machines) that lately has been embraced and promoted by many small to large players who provide diverse IT monitoring and analytics tools and expertise; e.g. see IBM's Youtube videos about advantages with Predictive Maintenance or our Youtube video on 'The Big Basic Questions in Managing Biometric Applications'.

Scope of proposed project

We sense the time is finally ripe to raise the awareness and equip the biometric users with the framework and tools with which they can use a common language to set minimum quality requirements and deploy associated monitoring and control mechanisms. A standard for improving four of fundamental properties of any biometric application: **Reliability**, **Availability**, **Maintainability**, and **Performance.** Add to that keeping operational costs (such as maintenance or downtime) at a minimum *too*.

Operational Monitoring is to use real-time (or offline but real-world) data to detect, diagnose, report, and recover issues in order to ensure that end-customers' business goals and requirements are met or exceeded. An Operational Monitoring program is concerned with the use of definitions, methods, and specialized tools to fulfill the said objective.

The project will deal with the following parts:

- Informative standards and their relevance
- Terms and Definitions
- What is Biometrics Operational Monitoring?
- Why is Biometrics Operational Monitoring needed?
- Three distinct goals of Biometrics Operational Monitoring
- Five steps towards implementing and adopting a successful Biometrics Operational Monitoring program
- What is Service Level Agreement (SLA) and why is it important?
- How to estimate biometrics operational costs
- Functions of general Biometrics Operational Monitoring tool
- Properties of general Biometrics Operational Monitoring tool
- Relationship between units/elements, events, alerts, and metrics
- Interface between the biometric system and the Biometrics Operational Monitoring tool Application Programming Interface (API)
- Q&A related to Reliability, Availability, Maintainability, and Performance in the context of BPM Example of metrics in a Service Level Agreement
- Sample Service Level Agreement
- Sample of symptoms and their possible causes
- Reference cases in applying Operational Monitoring in biometric applications. We currently have one reference case with IriTech's new cloud-based iris recognition service IriSecureID. We are in talks with other vendors to establish more reference cases in order to have greater diversity in terms of biometric modalities and application type.

Annex/Base document and dedicated Web portal

Title: 'Best Practices in Biometrics Performance Monitoring Programs',
We warmly invite to view or download it at www.BiometricsPerformanceMonitoring.org

The white paper and its dedicated web portal focus on the use of standards, methods, processes, and IT tools to support end-users' and businesses' real-world expectations associated with Reliability, Availability, Maintainability, and Performance of biometric-based verification and identification systems and applications.

Why OASIS

We are very proud of OASIS and ourself *too* for we could early-on *see* the trend 'biometrics and web-services'. (we made it our backbone starting in 2003 when we found the company and the product).

We have mentioned the significance of OASIS initiatives and role in development of Web

services and biometrics-related standards in diverse places such as our website and Best Practices document and portal. We think OASIS is the optimum forum to initiate this standard (we mentioned SC37 in the Best Practices document but since then and two years of observation we shifted our vision more towards OASIS; we have not yet proposed it as an NWI to SC37).

Relevant links:

- Just released: Best Practices in Biometrics Performance Monitoring Programs
- 'There's A Metric for That': How 'Big Data' Impacts Biometrics Market and Industry
- LinkedIn survey: Real-time system monitoring a necessity in Border Management and Physical Access Control biometric applications
- BioUptime Gets Updated: Now Includes Performance Reports for Access Control Applications