Reliability, Availability and Maintainability in Biometric Applications

Delivering Quality of Service that customer wants

A WHITE PAPER

Version r1.0

Date of release: January 2, 2008

SWEDEN

OBL
OPTIMUM BIOMETRIC LABS

Introduction

First of all, thank you for your time and interest! We would like to bring to your attention three extremely important aspects in biometric applications: **Reliability, Availability** and **Maintainability (RAM).**

This document is intended for everyone with any current or prospective relation with biometrics in general and for those in charge of management of biometrics systems in particular. We have identified the following set of key functions across the entire value grid who may have great use of this document:

- ◉ **CIO** and **CSO** of end-user organization in charge of procurements, planning or specifying requirements on biometric applications
- ◉ **System administrator**, **Operator** and **First-line support** in charge of day-to-day maintenance and management of biometric applications
- ◉ **Third-part Evaluator** and **Advising Consultant** to end-user organizations
- ◉ **System architect** and **developer** in System integration companies
- ◉ **CTO** and **Product manager** of biometric product vendors and biometric service providers (BSPs)
- ◉ **Marketing** and **Sales managers** of Biometric product vendors, BSPs and system integrators

This document will explain fundamental basis of RAM in the context of biometrics; it is intended to be used as a guideline on what to consider and how to formulate base requirements and how to evaluate real-world performance metrics in order to support end-user business objectives to the fullest.

We will conclude with a list of clear-cut advantages for the value grid when RAM is seriously taken into account in planning and implementing a management program for biometrics systems.

> *Please note that:*
>
> ★ *In a separate and complimentary white paper we will introduce **Proactive Monitoring Program** as the key strategy on approaching and maintaining maximum Operational availability in mission critical biometric applications while minimizing Maintenance costs!*
>
> ★ *The **Operational Security** and **Usability** aspects of biometrics (system/user/usage-dependent) dealing with e.g. false accept, false reject and failure-to-enroll are outside the scope of this document and a topic for a separate white paper.*

"Biometrics never fail"

Simply not true! neither from the Security, Vulnerability and Usability perspectives nor the Reliability. In fact, biometrics need special care due to a group of factors that generally affect the overall system performance:

- ▶ Human factors:
    - – fraudulent activities such as intrusion etc.
    - – accidents
    - – configuration/maintenance caused issues
- ▶ External environmental conditions:
    - – light condition (*e.g.* face and iris)
    - – noise and vibration (*e.g.* voice)
    - – dirt, temperature, humidity (*e.g.* fingerprint)
- ▶ System related issues:
    - – hardware breaches and deterioration
    - – software failure
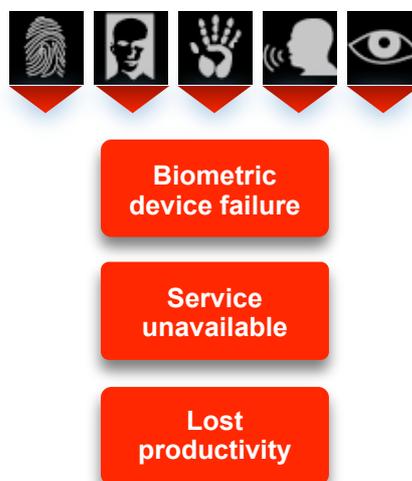
The example above illustrates one of the potential scenarios in which a business mission relying on biometrics would fail. With an optimum interplay achieved between culture, policy and technology (a holistic approach), scenarios like this are either early detected and recovered or ultimately prevented from ever occurring.

How to set Availability requirements

To define requirements for operational availability you can use the following industry-recognized terms and definitions that are fully applicable in the context of biometrics:

- **Downtime** is the total (accumulated) time in an observed or predetermined period of time that the biometric device/service is unavailable to users. Note that downtime, during the intended operating period, is calculated independently of its underlying reasons such as planned or unplanned shut-downs (due to e.g. maintenance, updates, power failures etc.).
- **Uptime** is the total (accumulated) time in an observed or predetermined period of time that the biometric device/service is available to users.

- **Operational Availability (A$_O$)** is the actual availability that the customer experiences. It is easily calculated by: uptime / (uptime+downtime)

Here we further clarify these terms by an example: ***Assume that your biometric service must serve 9 hours per day for 365 days per year and you allow for a maximum of 10 hours downtime annually. Then:***

> ***The calculated A$_O$ is 99.70% which can be used to set the required operational availability in a SLA contract.***

What is Reliability really

Reliability can be defined as the probability that a system, a sub-system or a component will operate successfully at a given time. The following metrics used in diverse industries are among indicators of reliability performance:

- **Mean-Time-Between-Failure (MTBF)** is the average time duration between failures of a functional entity under given conditions. It is typically applicable to entities that are "repairable", i.e. supposed to be fixed and then returned to operation.
- **Mean-Time-To-Failure (MTTF)** is the average time duration to the first failure of a functional entity under given conditions. It is only applicable to "non-reparable" entities where the entity is replaced with a new one.

Example: A supplier claims that its fingerprint sensor has a MTTF of 7300 hours.

☑ ***Hint: MTBF and MTTF are many times estimated using predictive analytical models. However:***

> ***True measures on MTBF or MTTF are always computed using collected data from real-world operations.***

How to set maintenance requirements

Maintainability can be defined as the probability of performing a successful maintenance action within a given time. It is measure of how fast a recovery action of a failed entity leads to operational status. The following metrics used in diverse industries are among indicators of maintainability performance:

- **Mean-Time-to-Recovery (MTTR)** is the average time it takes to restore an entity to operational status after it has failed to function. MTTR is also interpreted as Mean-Time-to-Repair/Replace/Resolve/Restore.

Note that with a MTTR of e.g. 1 hour the supplier does not guarantee an uptime (or even notification of the problem) within 1 hour. What the supplier states is that the recovery action is estimated to approach around 1 hour. Therefore, MTTR should not be used if the end-user requires guaranteed uptime, after a failure, within a given timeframe.

☑ ***Hint: Therefore, depending on a maintenance contract (typically in a SLA) the end-user usually want to hold the supplier accountable for maintenance.*** In this case it is much more useful to use:

- **Maximum-Time-to-Recovery** which is the maximum allowed time that includes taking a corrective maintenance action until the operational status is achieved.

> ***In a maintenance contract, where budget allows and nature of mission is critical, we recommend to use Maximum-Time-to-Recovery.***

Which maintenance strategy to apply

Assume that you are in charge of developing a maintenance program for a large number of biometric acquisition devices in a self-enrollment application where these devices are geographically placed in different zones across your site. How would you undertake this task?

First of all let us define and categorize maintenance of biometrics. Then we will point at some factors when considering which maintenance strategy to apply. Maintenance means any action such as operational performance monitoring, adjustment, configuration and restoration of an entity that is performing poorly, is near failure or has failed to operate as intended. Maintenance strategies are of following types:

- ✳ **Corrective (reactive) maintenance** is a recovery action performed after failure of a functional entity in order to restore it to its operational status.

- ✳ **Preventive maintenance (PM)** is performed periodically in order to reduce the probability of failure or deterioration of a functional entity.

- ✳ **Scheduled (routine) maintenance** is a preventive maintenance performed according to an established time schedule or a predetermined frequency of usage.

- ✳ **Predictive maintenance (PdM)** is to use past trends to predict failures. Also called Condition-based monitoring.

✺ **Proactive maintenance (Proactive monitoring)** is the latest, most popular and probably the most cost effective of all maintenance strategies since it selects the best of several maintenance methodologies with a holistic view of vigilance in mind. It is often interpreted and structured in slightly different ways depending on who advocate it and in which industry. The bottom line is: Proactive maintenance focuses on pinpointing and eliminating the root-causes rather than symptoms of failure. It makes use of e.g. continuos monitoring, analyzing, detecting, diagnosing and responding actions.

> *The main goal of Proactive monitoring is early detection and quick resolution before a failure leads to a major issue.*

Generally when considering which maintenance methodology to apply the following factors should be taken into account:

✦ The type of your biometric application:
  - Your requirement on the operational availability and the speed of recovery
✦ A detailed risk assessment of the supporting technologies and the infrastructure:
  - A detailed analysis of potential root-causes of failure
✦ Your maintenance budget and availability of staff
✦ The competence areas that should be covered in your organization
✦ The choice of technology to support your management/maintenance policy

A properly performed risk assessment should output prerequisites for developing a Maintenance Strategy Program which should be aligned with your business objectives and evaluated in a continuously measured Return on Investment (ROI).

> *Ultimately, your goal is to minimize the maintenance costs (reduce maintenance!) by implementing the most efficient maintenance policy and technology that maximizes uptime.*

Key Values

This document has analyzed and highlighted RAM from a value-added perspective. We conclude by summarizing the value-grid's objectives that perfectly match those of a fully exploited RAM.

End-user

✓ Minimize Total Cost of Ownership (TCO):
  • Reduce maintenance costs (Maintainability)
✓ Increase biometric uptime and maximize Quality of Service (Productivity)

Prime contractor (Service/Solution provider)

✓ Meet and exceed Service Level Agreement:
  • Measure and meet agreed A_0 and reduce downtime (Availability)
  • Improve Maximum-Time-To-Recover (Maintainability)
✓ Implement the most efficient management policy and technology to:
  • Early detect and eliminate root-cause of failure (Reliability)
  • Reduce operational costs (RoI-measured)
✓ Provide best possible end-user support

Biometric product vendor / BSP

✓ Consolidate operational performance feedback
✓ Optimize product performance (Reliability)
  • Improve MTTF/MTBF
✓ Increase competitive advantages

Useful sources

- ISO/IEC 2382-14 Information technology - Vocabulary - Part 14: Reliability, maintainability, availability
- ISO/IEC 27002:2005 - Information technology -- Security techniques - Code of practice for information security management
- The Transportation Security Administration (TSA), "GUIDANCE PACKAGE, Biometrics for Airport Access Control". (*ref.* 3.2 OPERATIONAL AVAILABILITY). URL: http://www.tsa.gov/assets/pdf
- The Construction Property Services Industry Skills Council in Australia (CPSISC), "Monitor biometrics equipment/systems" (*ref.* ELEMENT, PERFORMANCE CRITERIA). URL: http://www.cpsisc.com.au/projects/Biometrics%20Project/

Keywords: biometrics, operational availability, overall system performance, downtime, uptime, service level agreement, reliability, mean-time-between-failure, mean-time-to-failure, maintainability, mean-time-to-recovery, maximum-time-to-recovery, corrective (reactive) maintenance, preventive maintenance, scheduled (routine) maintenance, predictive maintenance, proactive maintenance, proactive monitoring, root-cause analysis, continuos monitoring